Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2007–2008

28 684 Naar een veiliger samenleving

Nr. 133 **BRIEF VAN DE MINISTER VAN JUSTITIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 14 april 2008

OVERZICHT

De samenleving maakt in toenemende mate gebruik van informatie- en communicatietechnologie. Digitalisering wordt ervaren als een vanzelfsprekende maatschappelijke ontwikkeling, die wenselijk en positief is. Tegelijkertijd kent digitalisering echter ook ongewenste, negatieve effecten. Dit heeft geleid tot verandering van wetgeving en verruiming van de bevoegdheden voor politie en justitie ten behoeve van de opsporing. Juist op het internet worden de negatieve effecten het meest zichtbaar. Deze brief bevat een beleidskader voor de rechtshandhaving bij cybercrime in het algemeen en internetmisbruik in het bijzonder. Dit kader kent de volgende hoofdlijnen die op korte termijn tot actie zullen leiden.

1. De publieke-private samenwerking bij de preventie uitgebouwd

Voorkoming van cybercrime is cruciaal. Door samenwerking kunnen burgers, bedrijven en overheid elkaar helpen risico's te onderkennen en te vermijden. Zo zullen meldpunten en voorlichting blijvend hun functie uitoefenen. Daarnaast kunnen publieke en private partijen kennis en informatie uitwisselen en gericht samenwerken. Deze nadruk op preventie bij cybercrime, die past in de intentie van het bredere project *Veiligheid begint bij voorkomen*[1], heeft in ander verband uitwerking gekregen.[2] Deze inzet zal de komende tijd worden versterkt . Verder is samen met andere departementen gestart met de door de Tweede Kamer gevraagde inventarisatie van bestaande voorlichtingscampagnes in het kader van het voorkomen van cybercrime.[3]

[1] Tweede Kamer, vergaderjaar 2007–2008, 28 684, nr. 119.
[2] Tweede Kamer, vergaderjaar 2007–2008, 26 643, nr. 103 (Veiligheidsbeleid Informatie- en communicatietechnologie).
[3] Tweede Kamer, vergaderjaar 2007–2008, 28 684, nr. 126.

KST117524
0708tkkst28684-133
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2008

2. Meer en andere inzet van politie en justitie

Er komt de komende jaren in een oplopende reeks extra geld voor politie en Openbaar Ministerie beschikbaar om de aanpak van cybercrime te intensiveren. Bestrijding van cybercrime vraagt om een andere wijze van werken, met andere methoden en technieken, waarbij het vanzelfsprekend wordt dat de politie in de internetomgeving werkt. Structurele voorzieningen zorgen ervoor dat politie en justitie ernstige kwesties als kinderpornografie en radicale uitingen systematisch aanpakken. Hiernaast zullen andere onderwerpen meer projectmatig doorgelicht worden zoals illegaal gokken, grootschalige auteursrechtinbreuken door illegaal uploaden en andere vormen van fraude. Naast deze proactieve werkwijze, komen er organisatorische voorzieningen opdat politie en justitie op adequate wijze op aangiften van cybercrime reageren (aangifteprocedure, deskundigheid, richtlijnen over wat een toereikende reactie vormt).
Om dit voor elkaar te krijgen zijn structureel en incidenteel extra gelden beschikbaar, waarmee de beschikbare capaciteit en deskundigheid een nieuwe impuls krijgt. Maar ook binnen de bestaande middelen van het OM en de politie zullen aanpassingen nodig zijn om te voldoen aan de eisen die voortkomen uit de ontwikkelingen in de cybercrime.

3. Internationale samenwerking versterken

Alleen met adequate grensoverschrijdende voorzieningen kan een effectieve strafrechtelijke aanpak van cybercrime tot stand komen. Een verdere verruiming hiervan bij grensoverschrijdende doorzoeking van een computersysteem wordt nagestreefd. Cybercrime is naar haar aard grenzeloos – daarom zijn voorzieningen nodig die de geografische beperking in de opsporing waar mogelijk opheffen.
Nederland investeert ook op andere aspecten in de bevordering van een internationaal gezamenlijke aanpak van cybercrime, zoals in een gemeenschappelijke benadering van het blokkeren en filteren van ongewenste informatie en de uitbouw van de wederzijdse rechtshulpverlening.

4. Juridische instrumenten actualiseren

Nodig is een actief optreden van politie en justitie tegen verboden communicatie op internet, zoals bij kinderpornografie, discriminatie, haatzaaien en het op grote schaal illegaal aanbieden van auteursrechtelijk beschermd materiaal. Aan de mogelijkheid om in opdracht van de overheid content van het internet te verwijderen wordt een belangrijke plaats toegedacht. Onontbeerlijk daarbij zijn effectieve juridische instrumenten. Van groot belang zijn daarom de conclusies van de nog dit jaar af te ronden analyse waarom dit onvoldoende van de grond komt.
In 2008 zullen verder de uitkomsten beschikbaar komen van een inventarisatie waarbij de politie, het OM en het NFI betrokken zijn. Daarin gaat het om onderkenning van eventuele manco's in de praktijk en de regulering van de opsporingsmogelijkheden bij cybercrime. Zo nodig krijgt dit een vervolg, samen met de al in gang gezette voorbereiding van wetgeving ter implementatie van internationale afspraken, zoals bijvoorbeeld zijn in het kader van de bestrijding van kinderpornografie.

5. Onderkennen en signaleren van ontwikkelingen

Veel informatie over de mate en vorm waarin cybercrime voorkomt, komt uit buitenlandse onderzoeken. Nog in 2008 wordt er gestart met een *nulmeting* voor de situatie in Nederland. Dit vormt de aanzet om in de toekomst meer structureel de vinger aan de pols te houden.

Deze vijf hoofdlijnen komen voort uit een analyse van de ontwikkelingen, het aanduiden van rechtspolitieke uitgangspunten voor de (straf)rechtshandhaving bij cybercrime, de uitwerking daarvan voor politie en justitie en een toespitsing op enkele belangrijke deelterreinen. Dit alles vormt de inhoud van de rest van deze brief. Over het onderwerp van deze brief, cybercrime[1], is recent een literatuuronderzoek van het WODC verschenen onder de titel *High-tech crime, soorten criminaliteit en hun daders: een literatuurinventarisatie*.[2] De resultaten hiervan zijn verwerkt in deze brief. Het verslag van het onderzoek, dat al aangekondigd is in de bovengenoemde brief over het project Veiligheid begint bij voorkomen, zend ik u hierbij ter kennisneming.

[1] In deze brief wordt aangesloten bij de terminologie die (onder andere) de Europese Commissie hanteert: «criminal acts committed using electronic communication networks and information systems or against such networks and systems» (Towards a general policy on the fight against cybercrime. Communication from the commission to the European Parliament, the Council and the Committee of the regions. 22 .5 2007) Andere termen die in dit verband (onderling inwisselbaar) gebruikt worden zijn «computercriminaliteit», «computergerelateerde criminaliteit», «high-tech crime». Zie ook de definitie die in kringen van de Verenigde Naties in gebruik is: «cybercrime is harmful acts committed from or against a computer or a network» (Working Group on Internet Governance; zie www.un.org). In de tekst geldt de term cybermisdaad als synoniem voor cybercrime.

[2] R.C. van der Hulst en R.J.M. Neve. WODCO&B nr. 264, High-tech crime, soorten criminaliteit en hun daders: Een literatuurstudie. Ministerie van Justitie/WODC, Den Haag, 2008.Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

I INLEIDING

De aanpak van cybercrime is onderdeel van het Beleidsprogramma 2007–2011 van het kabinet. In de brief over het project *Veiligheid begint bij voorkomen* staat als onderdeel van het thema «ernstige criminaliteit» een nadere aanduiding hiervan. Bij de behandeling van de Justitiebegroting, is aan uw Kamer toegezegd nader in te gaan op de rechtshandhaving bij vormen van misbruik (bijvoorbeeld kinderporno, uitingen van haat, alsook het oproepen tot terrorisme) zoals die zich op het internet manifesteren. De voorkoming en bestrijding van dergelijke verschijnselen zijn de afgelopen periode afzonderlijk in het overleg met de Tweede Kamer aan de orde geweest. Daarbij ontstaat telkens weer een discussie over de rol van de (strafrechtelijke) rechtshandhaving: waartoe dient deze, welke verwachtingen mag men op dat gebied koesteren en welke ambitie toont het kabinet in dit opzicht? Het lijkt zinvol om deze invalshoeken niet alleen per afzonderlijk fenomeen aan de orde te stellen, maar om dat in een meer algemeen kader te benaderen. Deze brief schetst een dergelijk breder kader. Tevens komt een op internet toegespitst opsporingsbeleid aan de orde en de verdere uitbouw daarbij van van opsporings- en vervolgingscapaciteit in de komende jaren.

Allereerst komt aan bod de algemene maatschappelijke context waarin cybermisbruik en cybercrime spelen, waarna de uitgangspunten voor het beleid worden geformuleerd. Vervolgens komt de focus te liggen op de strafrechtelijke rechtshandhaving met aanduiding waar de investeringen plaatsvinden in aandacht en middelen. Daarna krijgen specifieke thema's aandacht, zoals kinderpornografie, radicalisering, illegaal gokken en auteursrecht.

II DE CONTEXT VAN CYBERCRIME EN RECHTSHANDHAVING

Een ander aangezicht

Met de doorwerking van de informatie- en communicatietechniek (ICT) in de samenleving verandert het aangezicht van de criminaliteit. De ICT maakt tegenwoordig deel uit van de *modus operandi* van de criminaliteit en vervangt (door technische ondersteuning vereenvoudigde uitvoering) een belangrijk deel van de «oude criminaliteit». Denk hierbij bijvoorbeeld aan illegale handel en ook aan financieel-economische criminaliteit. De omstandigheid dat veel sociaal en zakelijk verkeer via de ICT-infrastructuur loopt, biedt bredere mogelijkheden voor criminaliteit. Er is een ruimere gelegenheidsstructuur gevormd zoals de mogelijkheid om bedrog te plegen via veilingsites op internet (wel kopen niet betalen of wel incasseren en niet leveren). Anderzijds zijn er geheel nieuwe vormen van criminaliteit ontstaan waarbij ICT behalve middel ook expliciet doel is, ook al zijn deze vaak weer faciliterend aan andere, doorgaans financieel getinte vormen van criminaliteit (bijvoorbeeld *hacking*).
Rechtshandhaving was tot nu toe vooral georiënteerd op een fysieke werkelijkheid. De nieuwe werkelijkheid die door internet is ontstaan, kenmerkt zich door beperkte mogelijkheden tot rechtstreekse regulering, onduidelijkheid over wie waarop is aan te spreken en door een grote vluchtigheid. In de rechtshandhaving zal daarom naar nieuwe aangrijpingspunten moeten worden gezocht, bijvoorbeeld door oriëntatie op de verplaatsing van informatie in plaats van personen en goederen. Het Verdrag van Lanzarote, dat het verstrekken van creditcardgegevens aangrijpt om kinderporno op internet aan te pakken, is een goed voorbeeld van die nieuwe oriëntatie.

Aspecten

Er zijn vijf aspecten aan de ICT-invoering die in het bijzonder van belang zijn voor de cybercrime en de mogelijkheid daar in de rechtshandhaving tegen op te treden.

Ten eerste is er een steeds grotere afhankelijkheid van de ICT-voorzieningen en daarmee een verhoogde *kwetsbaarheid*. Een verstoring van de integere werking van die infrastructuur kan al snel vergaande consequenties hebben voor het functioneren van maatschappelijke sectoren of van ondernemingen.

Ten tweede heeft de communicatie via moderne middelen vaak een anoniem karakter: men kent elkaar vaak alleen via «elektronische communicatie» wat drempelverlagend kan werken voor onfatsoenlijk of schadelijk gedrag. De anonimiteit is des te sterker aanwezig omdat de «cyberidentiteit» niet altijd in overeenstemming is met de werkelijke identiteit van de afzender en daardoor niet of nauwelijks verifieerbaar. Er wordt gewerkt met aliassen en het aantal aangeboden hulpmiddelen om je op internet te begeven zonder dat er sporen van de eigen identiteit achter worden gelaten c.q. die de opsporing daarvan sterk bemoeilijken neemt toe.

Ten derde biedt de ICT de mogelijkheid om sociale en zakelijke transacties *massaal en snel* te verrichten. In verhouding daarmee is criminaliteit zónder ICT beperkt en traag. De potentieel aan cybercrime verbonden schade is daarom groot: er kunnen vele slachtoffers in één keer vallen, en tijd om daar eventueel nog op tijd een stokje voor te steken is er niet of zeer kort. Zo kunnen virussen (vaak langdurig) miljoenen slachtoffers maken, oplichting kan ook met een lage slachtofferkans nog succesvol uitpakken (1 promille van een miljoen benaderden is 1000 benadeelden). Sommige vormen van criminaliteit (als pogingen tot *phishing,* diefstal van identiteitsgegevens) meet men in aantallen per milliseconden. Deze massaliteit en snelheid, in combinatie met de grote mate van (mogelijke) anonimiteit, maken het moeilijk zicht te krijgen op de transacties. Tevens is het lastig te reconstrueren wat er zich precies heeft afgespeeld.

Ten vierde relativeert de ICT natuurlijk de grenzen tussen organisaties en landen. Het is in hoge mate arbitrair waar in elektronische netwerken fysiek (deel)bestanden zijn opgeslagen of langs welke paden gegevens stromen: dat kan in een eigen organisatie of land, maar even goed elders. Voor de rechtshandhaving, die traditioneel berust op het beginsel van *territoriale competentie*, leidt dit vanzelfsprekend tot complicaties.

Ten vijfde is er de veranderlijkheid in de toepassing van de ICT. De snelheid is toegenomen waarmee die techniek nieuwe toepassingsmogelijkheden schept die doorwerken in de organisatie van het maatschappelijke leven. Hiermee verandert het aangezicht van de cybercrime voortdurend. Internet schept telkens nieuwe gelegenheden voor de bestaande criminaliteit. Deze *permanente dynamiek* stelt natuurlijk eisen aan het organiseren van het voorkomen en bestrijden van de cybercrime. Dat zal alert mee moeten groeien met de veranderingen die de ICT oproept. Dit geldt ook voor de wet- en regelgeving.

Dader- en slachtofferschap

Wat betreft daderschap van cybercrime laat het hierbij gevoegde WODC-onderzoek zien, in overeenstemming met wat elders gevonden is, dat er weinig substantieels bekend is over de *kenmerken van daders*. Voor zover daar kennis over voorhanden is blijkt eerder van weinig toegespitste daderprofielen dan van nauwkeurig aan te geven eigenschappen van daders of van bendes. Dat is ook niet verwonderlijk. Cybercrime is feitelijk een paraplubegrip waaronder een verscheidenheid aan (vaak al langer bestaande) criminaliteitsvormen schuil gaat.

Net als bij klassieke criminaliteit blijkt (in de UK) in het algemeen een

oververtegenwoordiging onder de daders van jongens en jonge mannen.[1] In lijn hiermee komt uit het WODC onderzoek nadrukkelijk naar voren dat de hoofdmoot van cybercrime financieel gemotiveerd is en dus commune criminaliteit is. Elders is gevonden dat bij cybercrime soms het witte-boordengehalte relatief hoger ligt.[2] Daderprofielen lijken hiermee niet nadrukkelijk ICT-specifiek en bieden als zodanig geen sterke ankers voor het te voeren handhavingsbeleid. Als ingezoomd wordt op specifieke delictvormen blijkt er weinig kennis over daderkenmerken. Wel laat het WODC onderzoek zien dat de georganiseerde misdaad kansen heeft bij delicten als softwarepiraterij, internetfraude, witwassen, en handel in *botnets* en malware.

Wat betreft slachtofferschap in het jaar 2005 zou één op de 18 Amerikaanse huishoudens te maken hebben gehad met identiteitsdiefstal (6,4 miljoen gevallen), vooral door vals gebruik van een creditcard door derden. Hierbij is er niet een bepaalde groep huishoudens die eruit springt bijvoorbeeld in termen van leeftijd en inkomen.[3] Een algemene trend die ook het WODC-onderzoek aanstipt is dat criminele activiteiten in de toekomst vaker zullen worden afgestemd op een *specifiek doel*. Vooral slachtoffers die de technische kennis van digitale communicatiestructuren ontberen (waaronder veel ouderen) kunnen hiervan de dupe worden. Verder worden we steeds vaker geconfronteerd met materiaal op internet dat schadelijk kan worden geacht voor jongeren, zoals bijvoorbeeld games met een zwaar agressief karakter.

Ook ondernemingen die zaken doen via internet blijken niet zelden met criminaliteit te worden geconfronteerd, bijvoorbeeld met vormen van bedrog als oplichting en advertentiefraude.[4] Het is aannemelijk dat, gegeven het ICT-gebruik in Nederland en het eveneens hoge peil van zakelijke transacties via internet, ook in ons land het risico van slachtofferschap onder burgers en bedrijven breed aanwezig is. *«Cybercrime is in toenemende mate een probleem voor zowel de publieke als de private sector... Bij de overheid zijn vooral kleine gemeenten kwetsbaar»,* luidt een recente diagnose over de Nederlandse situatie.[5] Tevens is in ons land meer dan incidenteel sprake van slachtofferschap van kinderen en jongeren als het gaat om seksueel misbruik, om het pesten van medeleerlingen, om belaging. Nieuw daarbij is sinds enige tijd het met mobiele telefoons filmen van incidenten en het plaatsen van dat materiaal op internet.

Hiernaast zijn enkele vormen van cybercrime als «slachtofferloos» te kwalificeren. Deze maken inbreuk op collectieve belangen meer dan op individuele benadeelden. Voorbeelden zijn haatzaaien of bevordering van de ideologische grondslag voor terrorisme.

De relatie tussen daders en slachtoffers – «vertrouwen»

Kenmerkend voor veel sociale en vooral zakelijke ICT-contacten is het vluchtige karakter ervan. Communicatie geschiedt niet van gezicht tot gezicht maar door uitwisseling van signalen en symbolen op afstand. Dit geeft de sociale wisselwerking een anoniem karakter, wat nog versterkt wordt doordat velen niet de eigen naam gebruiken maar van een alias gebruik maken. Al langer is bekend dat de drempel om een ander onheus te bejegenen of te bedriegen lager ligt bij anonieme communicatie dan wanneer personen en ondernemingen elkaar – langer – kennen. Onder die omstandigheden is voorspelbaarheid van elkaars gedrag de basis voor wederzijds vertrouwen. Met het begrip «vertrouwen» is de voornaamste opgaaf van het ICT-gebruik gegeven: wil de informatie- en communicatietechniek zijn economische en sociale functie ten volle kunnen vervullen, dan zal voldoende vertrouwen aanwezig moeten zijn bij burger en bedrijven om daar veilig gebruik van te maken. Zo bleek een meerderheid van burgers zich – althans enkele jaren terug – zorgen te maken over veiligheid en vertrouwelijkheid van het zaken doen via ICT (*e-commerce*).

[1] Andere kenmerken doen er niet of minder toe; alleen bij «e-mail harassment» scoren meisjes ook hoog. Vooral het daderschap bij het schenden van auteursrechten breed verspreid (15% van ondervraagden), minder komt voor het anderen lastig vallen (10%) en zaken als productie van virussen, hacken en pesten via e-mails (0,7 – 0,9%). Fraud and technology Crimes: findings from the 2002/03 and British Crime Survey 2003 Edited by Debbie Wilson. UK: Home Office Online Report 34/05.

[2] De helft van gepakte en ingesloten stelers van identiteitsgegevens in de USA bestond uit personen die vergelijkbaar waren met veelplegende «straatcriminelen», maar de andere helft uit personen uit de middenklasse die zich met identiteitsdiefstal snel, makkelijk en risicovrij dachten financieel te kunnen scoren. Heith Copes and Lynne Vieraitis. Identity theft: Assessing Offenders' Strategies and Perceptions of risk. University of Alabama, Brimingham, June 30, 2007. Elders wordt identiteitsdiefstal ook nog verbonden met georganiseerde misdaad en terrorisme om hun misdaden te faciliteren. Francois Paget. Identity theft. MacAfee, White Paper, January 2007.

[3] Katrina Baum. Identity Theft, 2005. National Crime Victim Survey. Bureau of Justice Statistics, Special Report, US Department of Justice, November 2007. Hoewel er nuances zijn in de kans op slachtofferschap, is geen enkele groep hiervan gevrijwaard.

[4] Bijvoorbeeld: meer en meer doen mensen bestellingen via internet, ook bij kleinere bedrijven zoals bloemisten. In Australië wordt gemiddeld 32% van dergelijke bedrijven met creditcardfraude geconfronteerd, vaak meerdere keren. K. Charlton and N. Taylor. Online credit card fraud against small businesses. Australian Institute of Criminology. 2004.

[5] Trendrapport 2007 – cybercrime in trends en cijfers. Govcert.nl.

Zoiets remt het aangaan van transacties als het doen van bestellingen via internet.[1]

Omdat in de massaliteit van de ICT-interacties anonimiteit en vluchtigheid voorop staan, zullen bijzondere voorzieningen nodig zijn om het minimaal noodzakelijke vertrouwen op te wekken. *«We onderstrepen het belang van de veiligheid, continuïteit en stabiliteit van het internet en andere ICT-netwerken tegen dreigingen en kwetsbaarheden», «we zoeken naar het opbouwen van zekerheid en veiligheid in het gebruik van ICT door het vertrouwenskader te versterken»,* luidt dan ook de stelling die men internationaal omarmt.[2]

Adequaat meebewegen noodzakelijk

In de jaren '80 werd vastgesteld dat er nog geen concrete dreiging uitging van de computercriminaliteit, maar aanpassing van wetgeving werd wel nodig geacht om daar tijdig op te anticiperen[3]. In 1993 is de Wet computercriminaliteit I in werking getreden, in 2006 gevolgd door de Wet computercriminaliteit II. Inmiddels is cybercrime «gearriveerd» en de gevolgen daarvan zijn steeds meer zichtbaar in de samenleving.

Parallel aan de gewenning aan de nieuwe ICT-mogelijkheden die een belangrijke plaats innemen in ons dagelijks leven, is er noodgedwongen aandacht gekomen voor de schaduwzijden daarvan. Met gebruik van techniek en programmatuur zijn er filters tegen ongewenste berichten (*spam*) ontworpen, zijn brandmuren (*firewalls)* opgericht tegen aanvallen met virussen en andere ongewenste programma's en wordt geïnvesteerd vindt plaats in methoden om veilig via internet te kunnen betalen. De ICT-ontwikkeling gaat zo snel en is zo massief, dat de overheid op het gebied van de rechtshandhaving naast de al in gang gezette maatregelen extra dient te investeren in de komende periode.

III UITGANGSPUNTEN IN DE RECHTSHANDHAVING

Internationaal kader dominant

De aard van de cybercrime brengt met zich mee dat deze primair aandacht verdient op internationaal niveau. Alleen met adequate voorzieningen die de landsgrenzen overstijgen, kan een effectieve aanpak van het misbruik tot stand komen. Gelukkig is er op dat internationale vlak al veel gebeurd – dat geldt zowel de private sector, zoals in het bankwezen, als de aandacht die hiervoor is bij supranationale gremia. Hieronder is kort de stand van zaken weergegeven.

De *Raad van Europa* heeft zich al langer doen gelden als een belangrijke initiator om juridische randvoorwaarden te scheppen voor een goede aanpak van cybercrime. Dit geldt in het bijzonder de overeenkomst in strafbepalingen die noodzakelijk is om samen te kunnen werken, evenals strafvorderlijke bepalingen die van belang zijn voor de opsporing, de bewijsvergaring en de rechtshulpverlening.[4] Ook is het onderwerp van cybercrime nadrukkelijk geagendeerd bij de G8[5] en de OESO, die opriep te komen tot een cultuur van veiligheid in informatiesystemen.[6] De Verenigde Naties kennen sinds 11 november 2004 de *Working Group on Internet Governance* waaruit aanbevelingen voortkomen over de besturing van het internet betreffende kwesties die vitaal zijn voor een goede gang van zaken en die een evenwichtig optreden van private partijen en van overheden vragen.[7] Van bijzonder belang is natuurlijk de lijn die de Europese Unie volgt. Op 22 mei 2007 heeft de Europese Commissie een voorstel voor een algemeen beleid tegen cybercrime op tafel gelegd.[8] Hierin breekt de Commissie een lans voor een versterking van de samenwerking in de operationele rechtshandhaving en komt de klemtoon te liggen op de noodzaak van opleiding van politiële en justitiële functiona-

[1] Dit betreft het gemiddelde van Europese landen en de USA, waarbij Nederland opvalt door een betrekkelijk geringe terughoudendheid in het aangaan van ICT-transacties ook al ziet men net als in andere landen wel degelijk de risico's die daar aan zijn verbonden. Leon Cremonini and Lorenzo Valeri. Benchmarking Security and Trust in Europe and the US. Statistical Indicators Benchmarking the Information Society. Rand Europe, 2003.

[2] Working Group on Internet Governance, het rapport van «the third meeting» (citaat vertaald).

[3] Vergelijk de het rapport Informatietechniek en Strafrecht, van de Commissie Computercriminaliteit onder voorzitterschap van mr. H. Franken, april 1987.

[4] Counsel of Europe. Convention on cybercrime. Additional Protocol. Budapest, 23.XI.2001. Deze is mede ondertekend door de Verenigde Staten van Amerika.

[5] De G8's Subgroep on High Tech Crime, die zich bezig houdt met het beleid ter zake van de preventie van terrorisme en ernstige criminaliteit, veiligheid van grenzen en transport, bestrijding van computercriminaliteit en versterking van onderzoeken daarnaar, bestrijding van buitenlandse officiële corruptie en terughalen van gestolen nationale activa.

[6] Zie de aanbevelingen van de OESO op velerlei terrein zoals bescherming privacy en consumentenbelangen, zoals de «Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security» van 7 augustus 2002 (www.oecd.org).

[7] Working Group on Internet Governance, in het bijzonder het rapport van «the third meeting» (zie www.un.org) Hiernaast zijn er aanpalende activiteiten zoals omtrent fraude in de Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identitity, onder auspiciën van de Commission on Crime Prevention and Criminal justice (UN: Economic and Social Council).

[8] Towards a general policy on the fight against cybercrime. Communication from the commission to the European Parliament, the Council and the Committee of the regions. 22.5.2007.

rissen om de ontwikkelingen te kunnen blijven volgen. Tevens roept ze op de dialoog met het bedrijfsleven te verstevigen, zowel ter uitwisseling van informatie en inzichten, als in vormen van publiek-private samenwerking.

Ondanks het overheersende internationale karakter van cybercrime, richt de rechtshandhaving zich in Nederland uiteraard op wat op dat gebied in Nederland voorvalt en wat ons land daaraan kan doen, inclusief de daarbij te verlenen en te vragen rechtshulp. De bestaande samenwerking bij de bestrijding van criminaliteit met voor Nederland belangrijke landen wereldwijd zal zich ook steeds meer richten op de bestrijding van cybercrime. Nederland zal de komende jaren voortgaan met het actief ondersteunen van de inspanningen van Eurojust, Europol en Interpol op dit gebied. Daarnaast is het noodzakelijk om internationaal onderzoek naar de aard en omvang van cybercriminaliteit en naar daders en modus operandi van de grond te krijgen. Een van de mogelijkheden daarvoor zijn afspraken over een internationale onderzoeksagenda. Gekeken zal worden of andere landen daar aan mee willen doen. Als laatste punt kan genoemd worden de concrete verbetering van het internationale contact tussen de Nederlandse politie en OM en de landen in EU-verband door bilaterale en multilaterale uitwisseling van experts en informatie over casus en de «manier van werken».

Preventie en voorlichting voorop

Gegeven de omstandigheden, kan er niet voldoende nadruk liggen op de noodzaak tot zelfbescherming tegen cybercrime door burgers, ondernemingen en ook de overheid zelf. Het moet als het ware de zomerdijk zijn die voor de meeste gevallen van wassend water voldoende bescherming biedt. Daarnaast moeten preventieve middelen zorgen voor veiligheid van «*netwerken en informatie, het vermogen om tot een zeker niveau toevallige en kwaadaardige acties te weerstaan».*[1] Het kabinet heeft over deze noodzaak uw Kamer al vaker bericht[2]. Hiermee ligt er een grote (maar vanzelfsprekend niet onbeperkte) taak om zelf beveiligingsmaatregelen te treffen. Deze verantwoordelijkheid geldt in de eerste plaats de overheid zelf, die het goede voorbeeld moet geven in de beveiliging van de eigen systemen en vooral ook van het berichtenverkeer tussen burger en overheid. Ook geeft de overheid adviezen aan bedrijven en burgers. Zo helpt *govcert* om problemen in software en besturingssystemen op te lossen en waarschuwt bij virusaanvallen (www.govcert.nl). Digibewust biedt naast vele andere activiteiten, adviezen over *«bescherm jezelf, je kinderen, je computer en je bedrijf»* (www.digibewust.nl). Digibewust vormt een onderdeel van het bredere insafe network, wat opgezet is vanuit Safer Internet Plus.[3]
Een belangrijke rol is weggelegd voor internetproviders en andere internetpartijen als hostingbedrijven. Naast de,binnen hun eigen verantwoordelijkheid, zelf getroffen maatregelen zoals het opnemen van voorwaarden in gebruikersovereenkomsten en het blokkeren van kinderpornografie op internet, zijn bijvoorbeeld zorgplicht, aansprakelijkheid[4] en een vestigingsbeleid voor providers onderwerpen die de komende periode samen met de branche verder worden verkend. Een eventueel vestigingsbeleid zal echter alleen in internationaal verband tot stand kunnen komen gezien de Europese regelgeving op het gebied van Telecom.
In de auteursrechtsector doen rechthebbenden veel aan voorlichting gedaan om bij de burger een herbezinning te bewerkstelligen op het gevoel dat tegenwoordig alle content maar gratis is of zou moeten zijn en hun bewust te maken van het belang van auteursrechtbescherming.[5]
Evident is dat juist bedrijven die diensten via internet aanbieden een wezenlijke taak hebben in het verzekeren van een veilig ICT-gebruik. Zo dient bijvoorbeeld de financiële sector voor een veilig betalingsverkeer te

[1] De Europese Commissie in haar Network and Information Society: Proposal for a European Policy Approach (2001), met instemming geciteerd door de UN-Working Group on Internet Governance (citaat vertaald).
[2] Verwezen wordt ondermeer naar de brief van de Staatssecretaris van Economische zaken, mede namens de bewindslieden van Justitie, Binnenlandse Zaken en Koninkrijksrelaties en de Minister voor Bestuurlijke Vernieuwing over het eindadvies van het project National High Tech Crime Center (NHTCC) en het NPC-project Aanpak Cybercrime (NPAC). Recent heeft het kabinet aan de Tweede Kamer de gezamenlijke agenda op het gebied van het Veiligheidsbeleid Informatie- en communicatietechnologie aangeboden. (Tweede Kamer, vergaderjaar 2007–2008, 26 643, nr. 103). Beide brieven leggen de nadruk op preventie en de rol van voorlichting bij de voorkoming van cybercrime.
[3] http://ec.europa.eu/information_society/activities/sip/programme/index_en.htm.
[4] Zie Tweede Kamer, vergaderjaar 2005–2006, 26 671, nr. 20.
[5] Zie bijvoorbeeld www.auteursrecht.nl en www.bigweb.nl.

zorgen, en dienen elektronische marktplaatsen voorzieningen te bieden tegen bedrog. Uit recent onderzoek in Nederland blijkt evenwel dat ondanks een toename van het aantal incidenten bij zowel de private sector als de overheid een afname van het beveiligingsbewustzijn is te constateren ten opzichte van de afgelopen jaren.[1] Daarnaast constateren de onderzoekers een afname van het budget voor informatiebeveiliging.

Ook hebben ouders, net als in de «analoge wereld», de taak om kinderen te beschermen en voor te lichten, bijvoorbeeld om misbruik via babbelvoorzieningen (chatsites) tegen te gaan. Burgers hebben een eigen verantwoordelijkheid om niet naïef in te gaan op beloften van financiële verrijking of om blind geneesmiddelen via internet aan te schaffen. Natuurlijk: volledige risicomijding is niet mogelijk en ook niet nodig. Dat geldt voor sociaal en zakelijk verkeer in het algemeen, dus ook als die lopen via ICT-voorzieningen. Er zal evenwicht moeten zijn tussen de omvang van die risico's en wat de samenleving redelijkerwijs aan beschermingsmaatregelen mag verwachten. Daarin ligt een eigen verantwoordelijkheid die men niet kan en mag verwaarlozen. Verder dan het aangeven van het grote belang van de zelfbescherming door preventie hoeft het hier niet te gaan. In het kader van de uitwerking van de plannen zal hierover nog nader met het bedrijfsleven worden gesproken: immers het veiligheidsbeleid staat voor de komende jaren vooral in het teken van de preventie (door middel van het project *Veiligheid begint bij voorkomen*).

In de Tweede Kamer is tijdens de behandeling van de kabinetsbrief over het project *Veiligheid begint bij voorkomen* een motie aangenomen van het lid Cörüz[2] die de regering verzoekt om een inventarisatie te maken van bestaande voorlichtingscampagnes in het kader van het voorkomen van cybercrime en de Kamer te berichten of dit afdoende is. De uitvoering van deze motie is inmiddels samen met de Ministeries van Economische Zaken en Binnenlandse Zaken en Koninkrijksrelaties ter hand genomen. De verwachting is dat in de tweede helft van 2008 de Tweede Kamer nader bericht kan worden.

Overheid stelt en steunt

De private verantwoordelijkheid kent natuurlijk haar begrenzing. Allereerst geldt dat private belangen vaak wel, maar niet altijd parallel lopen met het algemeen belang van de samenleving. Dit geldt bijvoorbeeld bij een zeer vergaand gebruik van persoons- of verkeersgegevens door ondernemingen met als doel het tegengaan van misbruik en criminaliteit, of als sprake is van vormen van eigenrichting die zich niet verdragen met de wet. Hierin heeft de overheid de taak om wettelijke kaders te scheppen van wat wel en wat niet mag, waarbij het vanzelf spreekt dat de overheid meer verantwoordelijkheid op haar eigen schouders neemt naarmate ze de burger en de onderneming minder ruimte biedt om zelf adequate beveiligingmaatregelen te treffen.

Voorts geldt dat private partijen ieder afzonderlijk niet altijd voldoende in staat zijn om de risico's van misbruik en criminaliteit te overzien, en dus ook niet in staat zijn daar verstandig op te reageren, of dat ze de risico's wel zien, maar individueel niet in staat zijn actie te ondernemen. Hier bewijst publiek-private samenwerking goede diensten. Daarnaast kan onder andere met meldpunten de vinger aan de pols van de ontwikkelingen worden gehouden en actieve voorlichting over de risico's en de daarop te enten voorzorgsmaatregelen worden gegeven. De overheid kan hiermee «helpen opdat men zichzelf kan helpen». Voorbeelden hiervan zijn de experimenten die gestart zijn in het verband van de Nationale Infrastructuur ter bestrijding van Cybercrime (NICC) als het gaat om de informatieknooppunten in een aantal belangrijke (vitale) sectoren. Ook

[1] Onderzoek informatiebeveiliging bij Nederlandse organisaties 2007, Hintzbergen/Wannee Capgemini.
[2] Tweede Kamer, vergaderjaar 2007–2008, 28 684, nr. 126.

een onderwerp als kinderpornografie waarbij sprake is van grote maatschappelijke onrust krijgt gericht aandacht van de overheid.

Veiligheid en privacy – herdoordenking

Zowel in wat de private sector is toegestaan, als wat de overheid doet in het kader van de aanpak van cybercrime, speelt de discussie over veiligheid en privacy. Doorgaans ziet men deze twee begrippen als tegengesteld aan elkaar, zeker als het gaat om ICT-gebruik: criminaliteit voorkomen en bestrijden tegenover *Big Brother*. Dit komt nog scherper te liggen nu vormen van ICT-misbruik zich zo massaal en snel kunnen manifesteren, dat een corrigerende benadering achteraf niet gemakkelijk effectief kan zijn. Dan is de roep om een preventieve benadering van risico begrijpelijk, wat in de knel kan komen met «het recht met rust gelaten te worden». De vraag is dan, of de ontwikkelingen van ICT, waaronder begrepen de instrumentalisering van internet zoals bij gokken en vormen van fraude, niet een hernieuwde doordenking vordert van de betekenis van privacy in de moderne samenleving, met mogelijk aanpassing van opvattingen over wat de *civil society* inhoudt.[1] Op 17 januari 2008 is de Commissie *Veiligheid en persoonlijke levenssfeer,* onder voorzitterschap van mr. A.H. Brouwer-Korf, geïnstalleerd die de taak heeft hier licht op te werpen.

IV FOCUS EN INZET VAN DE STRAFRECHTELIJKE RECHTSHANDHAVING

IV.1 Prioriteiten

De strafrechtelijke handhaving (opsporen, vervolging, berechten en bestraffen) zal in het bijzonder inzet verdienen waar het algemeen belang dat vordert, of wanneer er particuliere belangen spelen die men niet zelf kan beschermen. Deze insteek zal door de digitalisering op zichzelf niet veranderen.

Het algemeen belang

Optreden is met voorrang geboden als criminaliteit de *democratische rechtsorde* bedreigt of ondermijnt. Hiervan is vooral sprake bij terroristisch handelen die mede met behulp van ICT-voorzieningen een grote uitwerking kunnen krijgen. Juist het brede karakter van radicaliserende uitingen vraagt om een krachtige reactie, zoals aangekondigd in het coalitieakkoord (zie hiervoor paragraaf V.2). Voorts vordert het algemeen belang, vanwege de grote afhankelijkheid ervan, een goede bescherming van de *vitale ICT-infrastructuur,* indien er sprake is van dreiging met terroristische (of criminele) motieven. Het is in het belang van de maatschappij om digitale verlamming te voorkomen of de daaruit voortkomende crisis te beheersen, of dat nu ontstaat door technisch falen of door moedwillig menselijk handelen. In het kader van de strategie Nationale Veiligheid/bescherming vitale infrastructuur wordt de continuïteit en de weerbaarheid van alle sectoren tegen ICT-verstoringen bevorderd, evenals een veilig ICT-gebruik (cybersecurity). Het laatste verwijst naar vitale sectoren, waar een goede werking verre uitstijgt boven particuliere belangen en de samenleving in haar geheel raakt. Zo kan de algemene veiligheid in het geding zijn als via internet wapens of niet goedgekeurd vuurwerk worden verhandeld. Of de volksgezondheid kan in gevaar komen door de verkoop van nepmedicijnen via het internet. Naarmate de algemene veiligheid of de volksgezondheid dit vereist, zal dat de nodige aandacht van politie en justitie dienen te krijgen.

[1] Charles Raab The future of privacy protection. Cyber Trust & Crime Prevention Project. Edinburgh University, June 4, 2004.

Het private belang 1

In het private domein komen de traditionele criminaliteitsvormen voor die ook zonder tussenkomst van ICT gepleegd kunnen worden, maar door het gebruik van ICT nieuwe uitvoeringsmogelijkheden hebben gekregen.
Mede door de mogelijkheid om onherkenbaar te zijn op internet is het makkelijker overschrijden van de normale fatsoensgrenzen (niet altijd strafbaar, maar wel onwenselijk) aan de orde. Bedreigingen, vormen van seksuele delicten, maar ook pesterijen vallen hier onder. Naast het gebruik van e-mailverkeer, is dit ook aan de orde in allerlei vormen van *chatten* en bijvoorbeeld binnen omgevingen als YouTube en Secondlife.
Het is hierbij van belang te constateren dat het negatieve gebruik van deze mogelijkheden slechts een zeer klein gedeelte is van het totale gebruik.
In eerste instantie kan zelfregulering vanuit de internetbedrijven een nuttig middel zijn om dit aan te pakken. Het strafrecht komt hier in beeld wanneer de criminaliteit de *lichamelijke en geestelijke integriteit en de vrijheid* van personen (en vooral: van kinderen) ernstig aantast. Hiervan is sprake bij vormen van geweldpleging (bedreiging, intimidatie, belaging) en seksueel misbruik (in kader van kinderpornografie, *grooming*).

Het private belang 2

Het private belang speelt ook in de sfeer van *eigendom en vermogen*: de wereld van diefstal, inbreuken op auteursrechten, oplichting, fraude en vernieling. Kwantitatief is dit waarschijnlijk het meest omvangrijke domein van cybercrime, waarbij het vaak om op zichzelf betrekkelijk geringe schade per slachtoffer gaat maar wel om een groot aantal slachtoffers waardoor het totale bedrag tot omvangrijke benadeling leidt. Juist op dit terrein mag veel verwacht worden van zelfbeschermende maatregelen, reden om het strafrecht en de opsporingscapaciteit die daarvoor beschikbaar is, hier niet ten volle op in te zetten, maar geconcentreerd op specifieke situaties. Daarbij gelden twee criteria. De eerste is de relatieve omvang van de schade, gerelateerd aan de breedte van de schouders van de private partij zodat in het bijzonder zwakkere partijen strafrechtelijk bescherming genieten.[1] Het tweede criterium is de wijze waarop het delict wordt gepleegd in termen van doortraptheid, grofheid en stelselmatigheid: dit slaat terug op het beginsel dat men zich soms onmogelijk tegen de criminele bedreiging kán wapenen en er dus een rol voor de overheid ligt. In het bijzonder geldt dit wanneer de cybermisdaad georganiseerd plaatsvindt zoals bij internet- en identiteitsfraude of bij stelselmatige oplichting. Als vanzelfsprekend ziet de overheid de stijging van de aandacht van de georganiseerde criminaliteit voor het internet als een belangrijk aandachtsgebied. De aanpak hiervan zal in het verlengde liggen van de al bestaande aanpak van de georganiseerde criminaliteit en de intensivering daarvan via het project *Veiligheid begint bij voorkomen*.

IV.2 Inzet politie en justitie

Adequate reactie op melding en aangifte

De voorgaande prioritering in de aandacht van politie en justitie heeft betekenis voor de wijze waarop deze instanties reageren op meldingen (al dan niet via daartoe ingerichte overheids- of particuliere meldpunten) en aangiften. Daarvoor is een beleid geformuleerd in de zgn. *Aanwijzing voor de opsporing* (Stcrt. 2003, 41), waarin staat hoe men dient te handelen en onder welke omstandigheden van opsporingshandelingen kan worden afgezien. Het College van procureurs-generaal is gevraagd om te bezien of deze aanwijzing wijziging of aanvulling behoeft gegeven de kenmerken van de cybercrime. Meer in den brede is aan het College van procureurs-generaal gevraagd om – in het continue proces van de periodieke besluit-

[1] Sterkere partijen zijn immers meer in staat risico's te overzien, en kunnen meer meebrengen om zich tegen de gevaren te wapenen. Dit volgt het algemene uitgangspunt van het Wetboek van Strafrecht, dat dient om zwakkere partijen en belangen te steunen met the rule of law.

vorming over verlenging en aanpassing – de beleidsregels voor de opsporing en vervolging te onderzoeken op hun toepasbaarheid voor internet en de digitale omgeving.

Veel opsporingscapaciteit zal nodig zijn om toereikend te acteren op basis van meldingen c.q. aangiften van betrokkenen. Een toereikende reactie op melding en aangifte van cybercrime veronderstelt een organisatie die daarop is toegesneden. Hiertoe zal de politie in de komende jaren investeren in het stroomlijnen en professionaliseren van het aangifteproces als het gaat om cybercrime. Aangifte doen via internet is daar een belangrijk onderdeel van. Verder is er een basis nodig aan kennis en vaardigheden over de technische en strafvorderlijke aspecten van cybercrime om in voorkomende (doorsnee)gevallen op te kunnen treden. Dat geldt het goed opmaken van ook technische componenten in een proces-verbaal van aangifte, maar ook bijvoorbeeld dat men weet wat bij doorzoeking of inbeslagneming van belang is voor een goede waarheidsvinding. Hiertoe is investering in den brede voorzien in de opleiding en bijscholing van politie en justitie (OM en rechters) in het kader van *Veiligheid begint bij voorkomen*.

Belangrijk aspect van adequaat optreden bij melding en aangifte is de snelheid van optreden. Informatie die op internet verschijnt wordt in zeer korte tijd gekopieerd en op diverse plaatsen op het internet gezet. Hoe sneller politie kan optreden tegen een bepaalde site, film, of ander (beeld) materiaal, hoe minder kans op veelvuldig kopiëren is en hoe minder schade daardoor ontstaat. Het spoedeisend karakter van internet vergt met andere woorden snel en voortvarend handelen door de opsporingsdiensten.

Surveillance, thematische insteek

Naarmate de in het geding zijnde belangen sterker wegen, en naarmate minder vertrouwd kan worden op het verkrijgen van signalen betreffende cybercrime door daartoe aangedragen informatie uit de samenleving, zal de overheid zich meer moeten inspannen om die informatie te halen door actief te zoeken door middel van surveillance of in andere gevallen via monitoring.[1] Omdat dit een intensieve werkwijze is en dus veel aan capaciteit vraagt, is gekozen voor een tweesporenaanpak.

Enerzijds wordt de surveillance en monitoring op landelijk niveau gecontinueerd bij enkele vormen van cybercrime: dit geldt de al jaren bestaande surveillance op de Nederlandse markt van kinderpornografie, en op de verspreiding van radicaliserende boodschappen. Anderzijds krijgt de surveillance een thematische, projectmatige poot. Hierbij zullen politie en justitie op grond van externe signalen en een risicoafweging inzoomen op bepaalde onderwerpen (zoals vormen van cyberfraude, grootschalig illegaal uploaden van auteursrechtelijk beschermde werken of de markt van illegaal vuurwerk tegen het einde van het jaar). Om dat voor elkaar te krijgen komen er een beperkt aantal proeftuinen op bovenregionaal niveau. Dit krijgt in 2008 nadere uitwerking, inclusief toedeling van daartoe benodigde extra middelen, als onderdeel van het *Versterkingsprogramma bestrijding cybercrime*.
Vanuit dit landelijke, bovenregionale niveau zal de verbinding voortgezet en versterkt worden met de buitenwereld van bijvoorbeeld providersorganisaties, auteursrechtelijke (handhavings) organisaties, meldpunten en buitenlandse strafrechtelijke instanties. Tevens is er een logische aansluiting met het op nationaal niveau sinds 2007 opererende team *High Tech Crime* bij het Korps Landelijke Politiediensten. Deze verbinding helpt bij het verkrijgen en delen van nieuwe kennis voor de preventie en voorlichting.

[1] Onder surveillance wordt in dit verband verstaan: het op structurele en systematische wijze zoeken naar, en gericht volgen van bepaalde sites en activiteiten, personen en groepen ten behoeve van een keuze of operationele maatregelen getroffen moeten worden en zo ja, welke maatregelen het meest wenselijk zijn. Onder monitoring wordt in dit verband verstaan: het op structurele en systematische wijze volgen van uitingen en gedragingen op het internet waarmee inzicht wordt verkregen ten behoeve van beleidsvorming en -evaluatie, zonder gebruik te maken van bijzondere bevoegdheden.

Het voordeel van het starten op bovenregionaal niveau is dat dit betrekkelijk snel kan gebeuren. Wel zal in de toekomst voortdurend de afweging nodig zijn of internationale, nationale, bovenregionale of regionale actie gewenst is. Die afweging krijgt steun van de ervaringen die zullen voorkomen uit het werken in de genoemde proeftuinen: daarmee zullen *best practices* worden verkregen die ter lering strekken van de gehele organisatie van politie en justitie.

Geldelijke investering in capaciteit en kwaliteit bij politie en justitie

Voor een versterking van de aanpak van cybercrime door politie en justitie is binnen het programma *Veiligheid begint bij voorkomen* extra geld beschikbaar gesteld. Deze impulsen vormen een fors extra op wat nu daarvoor beschikbaar is aan capaciteit en kwaliteit. Versterking is voorzien zowel op regionaal als op bovenregionaal/landelijk niveau. Dit sluit aan bij de aard van cybercrime, die soms alleen lokale kenmerken heeft, maar die vaak ook internationale aspecten kent die samenwerking met één of meer instanties in het buitenland nodig maakt. Vaak zal cybercrime een betrekkelijk eenvoudiger kwestie vormen die men zonder specifieke ICT-kennis kan aanpakken, soms zal daar juist uitbundig inschakeling van bijzondere deskundigheid nodig zijn. De ene keer kunnen politie en justitie het zelf af, de andere keer zal inschakeling van private instanties zoals internetproviders of telecommunicatiebedrijven of gespecialiseerde private bedrijven aan de orde zijn.

Dit diverse karakter van cybercrime noopt tot een organisatie van de strafrechtelijke handhaving die in staat is samenhangend «van wijk tot wereld» te werken, waarbinnen men soepel en snel schakelt tussen het (inter)nationale en het (inter)regionale/lokale niveau. Het komt immers veelvuldig voor, dat een kwestie die lokaal begint mede op (intern)nationaal niveau aanpak vereist. En andersom: een buitenlandse signalering van virusverspreiding kan uiteindelijk slechts een lokale aanpak van een jongere in Sneek vorderen.

IV.3 Methoden

De aard van cybercrime (massaal, snel, anoniem, veranderlijk, grenzeloos) vraagt om een doordenking van de manier waarop daar tegen ingegaan kan worden vanuit het strafrecht. Soms kan een aangrijpingspunt gevonden worden door een informatiestroom te doorbreken (blokkering, filtering), soms door bijzondere opsporingsmethoden toe te passen, soms door het vragen of verlenen van rechtshulp. Dat komt in deze paragraaf aan de orde, maar zal ook verderop bij de specifieke thema's terugkeren. Zo is bij het tegengaan van illegaal gokken op internet gekozen voor een rem op het daarbij noodzakelijke financiële verkeer via banken en creditkaartmaatschappijen.

Notice-and-Take-Down, filteren en blokkeren

Bij het tegengaan van onrechtmatige content op het internet wordt een onderscheid gemaakt tussen Notice-and-Take-Down (NTD), blokkeren en filteren.
Onder NTD wordt in dit verband verstaan het op verzoek of op bevel van derden ontoegankelijk maken van bepaalde informatie op het internet door providers of andere internetpartijen[1]. Bij het NTD-verzoek (dus het ontoegankelijk maken op basis van vrijwilligheid) spelen de internetpartijen al een actieve rol: er zijn procedures waarbij klanten of internetgebruikers kunnen ageren tegen (vermeend) onrechtmatige uitingen. Een goed voorbeeld hiervan is YouTube, waar door middel van een eenvoudig signaleringssysteem («flagging») gebruikers de eigenaars kunnen atten-

[1] Met «andere internetpartijen» moet gedacht worden aan allerlei gespecialiseerde dienstverleners op het internet zoals data-centra, co-located hostingbedrijven, veilingsites, etc.

deren op misstanden. Meldingen van misstanden kunnen worden gedaan door individuele gebruikers, maar ook belangengroeperingen hebben hier een belangrijke rol op zich genomen.[1] Ook politie en justitie kunnen de internetpartijen hier op wijzen. Dergelijke signalering heeft vaak een positieve actie tot gevolg: de providers spelen hiermee al een belangrijke rol op grond van een zelf gevoelde verantwoordelijkheid. Deze vorm van zelfregulering verdient de voorkeur boven overheidsdwang.
Onder verantwoordelijkheid van het NICC wordt onderzocht op welke wijze de NTD-procedure, gebaseerd op publiek-private samenwerking, kan worden gestroomlijnd en efficiënter gemaakt.[2] Binnen de kaders van dit project wordt nu vanuit het bedrijfsleven een voorstel voor een NTD-gedragslijn gelanceerd en een structureel overlegplatform voor betrokken overheden, particulieren en bedrijfsleven. Nog vóór de tweede helft van 2008 zullen de resultaten beschikbaar zijn van dit NTD-project van het NICC.

De voorgestelde NTD-gedragslijn is bedoeld voor in Nederland gevestigde internetpartijen. Het verdient de voorkeur dat ook in het buitenland wordt bevorderd om een dergelijke NTD-structuur op te zetten. De bron van veel informatie ligt veelal buiten onze landsgrenzen hetgeen de noodzaak tot vergelijkbare NTD-methodieken in internationaal verband bevestigt.

Indien noodzakelijk, kan de officier van justitie een NTD-bevel geven, bijvoorbeeld wanneer de beoordeling of er sprake is van strafbare gedragingen leidt tot verschillende inzichten bij de private en publieke partij. De desbetreffende procedure is geformuleerd in artikel 54a van het Wetboek van Strafrecht, waarin staat dat een provider niet aan vervolging bloot staat voor het doorgeven van verboden boodschappen, indien hij voldoet aan het bevel van de Officier van justitie (daartoe gemachtigd door de rechter-commissaris) om voldoende maatregelen te nemen om die informatie ontoegankelijk te maken. Dit artikel is niet vanzelfsprekend een makkelijk en snel toepasbare manier om tot verwijdering van ongewenste of strafbare informatie te komen. Ook een juridische analyse van de Universiteit van Tilburg wijst op knelpunten.[3] De onderzoekers menen dat er vragen bestaan over de wettelijke basis voor een NTD-bevel. Deze analyse wordt meegenomen in het aanscherpen van de wettelijke instrumenten (zie verderop).

Met filteren en blokkeren wordt bedoeld het op verzoek van de politie onbenaderbaar maken door internet service providers (ISP's) voor haar klanten van bepaalde, veelal uit het buitenland afkomstige onrechtmatige informatie. In hoofdstuk V.I over de aanpak van kinderpornografie wordt hier nader aandacht aan besteed.

Overigens zal de effectiviteit van maatregelen als ontoegankelijkmaking of filtering bepaald niet altijd succesvol zijn. Zo kan informatie in razend tempo gekopieerd en via andere (minder toegankelijke) kanalen aangeboden worden.
Het blokkeren van bepaalde domeinen kan bovendien disproportionele gevolgen hebben; nietsvermoedende en onschuldige internetbedrijven kunnen worden afgesloten bij het *offline* halen van een compleet domein. Een afweging mede gericht op criteria van proportionaliteit en subsidiariteit is dan aan de orde, waarbij de aantekening dat een dergelijke beslissing bewust moet worden genomen opdat zo nodig verantwoording daarover kan worden afgelegd. Om te voorkomen dat een actie tot filtering of blokkering onnodig een brede uitwerking heeft, geldt als uitgangspunt dat beslissingen daartoe op een «laag niveau», maatgericht worden genomen, dicht bij de aanbieder van de informatie.

[1] Denk hierbij aan partijen als de Stichting Brein of het Meldpunt Discriminatie.
[2] De Stuurgroep Internet en Terrorisme heeft NICC specifiek opdracht gegeven hierbij specifiek te kijken naar een NTD-systematiek voor haatzaaisites.
[3] M.H.M. Schellekens, B.J. Koops en W.G. Teepe. Wat niet weg is, is gezien. Een analyse van art. 54a Sr in het licht van een Notice-and-Take-Down-regime. Universiteit van Tilburg, oktober 2007.

Bijzondere opsporingsmiddelen

Het is goed periodiek na te gaan of de regeling van de bestaande bevoegdheden als observatie, infiltratie, pseudokoop, pseudodienstverlening, stelselmatige informatie-inwinning, betreden van een besloten plaats en opnemen van vertrouwelijke communicatie met een technisch hulpmiddel voldoende aansluit bij de (technische) omstandigheden van heden en van morgen.
Gestart is met een inventarisatie naar de desbetreffende wet- en regelgeving, waarbij het Openbaar Ministerie en de opsporingsinstanties zijn betrokken. Op grond van de uitkomsten zal ik het nut en de noodzaak van aanpassing in de wet en regelgeving overwegen. Hierbij zal betrokken worden de uitkomst van het 2005 verrichte onderzoek van het NFI naar de (technische) mogelijkheden voor de opsporing op internet van kinderpornografie, waarover ik uw Kamer heb bericht.[1] Dit onderzoek wordt herhaald en verbreed naar het totaal aan opsporingsmogelijkheden op internet.
Deze exercities, waarin het zoeklicht komt te staan op de belangrijkste opsporingsmethodes en hun toepasbaarheid in de digitale omgeving, starten dit jaar. Mede in gang is gezet de wetgevingsvoorbereiding op basis van internationale afspraken zoals op het vlak van de bestrijding van kinderpornografie. Tevens krijgen de procedures aandacht waarin de bestaande regelgeving toepassing krijgt, zoals de wijze waarop in individuele gevallen de rechter tijdig betrokken is bij besluitvorming. Gezien het grenzeloze karakter van het internet zal hierbij tevens gekeken worden naar de internationale ontwikkelingen, zoals de uitspraak van het Duitse Bundes Verfassungs Gericht van 27 februari 2008[2] over de wettelijke toelaatbaarheid van «online Durchsuchungen».
Het resultaat van de hier benoemde inspanningen zullen mij naar verwachting in de tweede helft van 2008 bereiken.

De internationale dimensie

Het strafrecht is territoriaal gedefinieerd: de bevoegdheden van politie en justitie beperken zich tot Nederland, althans tot de gebieden waar de Nederlandse staat rechtsmacht heeft. Dat levert spanning op met het grenzeloze karakter van de moderne ICT-voorzieningen. Zo kan bij een doorzoeking van een computersysteem van een verdachte al snel de vraag rijzen of bestanden die men tegenkomt wel fysiek in Nederland aanwezig zijn. In de jaren '80 suggereerde de Commissie Computercriminaliteit in dit verband de wenselijkheid van het criterium van *beschikbaarheid:* een doorzoeking en benutting voor bewijsdoeleinden zou zich uit moeten kunnen strekken tot systemen en gegevens waar de verdachte legitiem toegang toe heeft, óngeacht waar en onder wie die systemen en gegevens berusten. Door de Raad van Europa is naar analogie een beschikbaarheidscriterium geformuleerd, zij het dat dit zich slechts uitstrekt tot het eigen nationale territorium.[3] De vraag dringt zich steeds sterker op, of het vasthouden aan het territoriale uitgangspunt houdbaar zal blijven. Deze materie is besproken in het verband van de totstandkoming van het *Cybercrimeverdrag* maar heeft niet geleid tot nadere regeling voor grensoverschrijdende netwerkdoorzoeking. Wel is helder geworden dat het zonder meer is toegestaan voor het publiek ter beschikking gestelde informatie in het buitenland op te halen en te benutten. Voorts kunnen gegevens uit een buitenlands systeem benut worden indien dat geschiedt met toestemming van de persoon die daartoe rechtmatig toegang heeft, zoals door het verstrekken van toegangscodes of door het feitelijk openen van de verbinding.[4]
Het lijkt onvermijdelijk dat ook buiten het eigen nationale territorium het criterium van beschikbaarheid wordt gehanteerd, op straffe van een

[1] Brief van de minister van Justitie d.d. 21 maart 2006 inzake NFI-Onderzoek Opsporing Kinderpornografie op internet (Just5399943/506).
[2] BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 – 333).
[3] Iedere deelnemende staat zal *«wettelijke en andere maatregelen ... treffen die nodig zijn om te verzekeren dat wanneer zijn autoriteiten zoeken in een ... bepaald computersysteem ... en reden hebben aan te nemen dat de gezochte gegevens opgeslagen liggen in een ander systeem binnen zijn territorium, en als zulke gegevens wettelijk toegankelijk zijn vanuit het systeem waarin gezocht wordt, die autoriteiten hun zoeken voortvarend kunnen uitbreiden naar dat andere systeem».* Convention on cybercrime, Title 4, Article 19 (eigen vertaling).
[4] H.W.K. Kaspersen, Bestrijding van cybercrime en de noodzaak van internationale regelingen. Justitiële Verkenningen, 30(8):58–75, 2004.

achterblijvende handhaving. Ik zal me daarvoor inzetten in internationaal verband.

Daarnaast is de *internationale rechtshulp* van groot belang. Niet altijd is rechtshulp of samenwerking opsporings- en vervolgingsautoriteiten daadwerkelijk mogelijk. Vanuit het uitvoerend niveau wordt aangegeven dat de samenwerking met een aantal voor de bestrijding van cybercrime belangrijke landen nog verre van optimaal of onmogelijk is. Naast de bestaande kanalen is er ook behoefte aan samenwerking met landen waarmee dat tot op heden weinig zo niet gebeurt. Als voorbeeld mag gelden Rusland. De eerste stappen om te komen tot samenwerking worden momenteel in gang gezet. Het laatste halfjaar is er informatie gewisseld over een aantal in Nederland lopende opsporingsonderzoeken. Het overdragen van deze zaken naar de autoriteiten in Rusland is op dit moment in een vergevorderd stadium. Zoals hierboven al is vermeld ziet Nederland Eurojust, Europol en Interpol als belangrijke partners bij de bestrijding van criminaliteit, inclusief de bestrijding van cybercrime. Verwacht mag worden dat ook zij breder op de wereld de samenwerking zullen zoeken en nader vorm zullen geven.

V SPECIFIEKE ONDERWERPEN

Binnen de algemene beleidslijnen zoals die zijn geschetst, krijgen hieronder enkele belangrijke en actuele kwesties nadere uitwerking.

V.1 De aanpak van kinderpornografie en seksueel kindermisbruik

Ontwikkelingen

De ICT heeft de markt van de kinderpornografie sterk veranderd.[1] Van oudsher was de markt in kinderpornografie een kleinschalige, waarin naast tijdschriften foto's, video's en tekeningen werden uitgewisseld. Nu is het een grootschalige markt met commerciële trekken[2], betrokkenheid van georganiseerde misdaadgroepen[3] en explicieter kindermisbruik in het bijzonder in derde wereldlanden[4]. Het aantal meldingen van kinderpornografie op internet en via andere elektronische kanalen in Nederland is de afgelopen jaren gestegen naar ruim 6400 in 2006[5]. De meldingen hebben voor het overgrote deel betrekking op specifieke websites met daarop kinderpornografische afbeeldingen. Verder gaat het vooral over meldingen van ongevraagde blootstelling via *spam* en e-mailberichten. De bron is doorgaans afkomstig uit het buitenland, in meerderheid van buiten de EU. Ervaringsdeskundigen wijzen verder op de toename van het belang van *chatsites* (inclusief de toename van fora en groepen binnen een specifieke site). Kindermisbruikers maken vaak gebruik van het internet om kinderen te lokken naar misbruikrelaties (*hawking*, *grooming).* Pedoseksuele avances lijken meer dan incidenteel voor te komen. Buitenlandse bronnen noemen een orde van grootte van 20% van de kinderen die chatrooms gebruiken en ongewenst benaderd zijn. In Nederland zou dit ook op 10–20% liggen.[6] Gelukkig zijn kinderen hierop steeds meer bedacht, mede als gevolg van voorlichting. Net zoals bij de benadering in de analoge wereld weigeren zij doorgaans in te gaan op dergelijke initiatieven. De overlap tussen misbruik en interesse voor kinderpornografie is fors.[7] Hierbij is dan van belang dat, waar vroeger er nog een zekere drempel bestond (men moest daadwerkelijk bij derden op zoek naar illegaal fotomateriaal en videobanden) nu met het gebruik van internet het verkrijgen van kinderpornografie is vergemakkelijkt. Dat maakt dat bij personen met een latente belangstelling voor kinderpornografie deze nu makkelijker wakker wordt gemaakt dan voorheen. Vanachter het toetsenbord kan wereldwijd worden gezocht. Juist de anonieme elektronische

[1] W. Ph. Stol, Kinderporno op intern. Zie: www.wodc.nl onder «aanpak criminaliteit».

[2] «De kinderpornografie die in Nederland is aangetroffen bestaat voor het grootste deel uit amateuristisch materiaal, vermoedelijk gemaakt door ontuchtplegers voor privé-bezit, maar van lieverlee toch in het commerciële circuit geraakt». Albert Benschop, Kinderporno in cyberspace, www2.fmg.uva.nl/sociosite/websoc.

[3] John Carr, Children and Technology Unit, NCH. London. Theme paper on Child Pornography for the 2nd World congress on Commercial Sexual Exploitation of Children (UNICEF, Yokohama, 17–20 December 2001).

[4] Hiernaast is het met behulp van de moderne (computer) technologie steeds gemakkelijker om een realistische afbeelding van een niet bestaand kind te vervaardigen of om aan een bestaande afbeelding van kinderen seksuele elementen toe te voegen. Deze virtuele of gemanipuleerde kinderpornografie is als «namaak» vaak nauwelijks meer van «echt» te onderscheiden. S. van der Zee en C. Groeneveld. Kinderpornografisch beeldmateriaal. Gepubliceerd in van Wijk, Bullens en van den Eshof; Facetten van zedencriminaliteit. Den Haag, Reed business information, 2007, blz. 229–247.

[5] Jaarverslag 2006 van de Stichting Meldpunt ter Bestrijding van Kinderporno op internet. Amsterdam, juni 2007.

[6] Engeland, USA zie Benschop, op. cit.

[7] Zo was 55% van de wegens bezit van in de kinderpornografie gearresteerden in de USA alleen een «bezitter», 40% waren duale delinquenten die zowel porno bezaten én kinderen misbruikten, 15% bezaten porno én probeerden kinderen te lokken via internet. Janis Wolak, David Finkelhor and Kimberley J. Mitchell. Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings from the National Juvenile Online Victimization Study. National Centre for Missing & Exploited Children. 2005.

verspreiding met zijn karakter van afstandelijkheid *(desensitivering*) kan mede aanleiding geven tot (verder) feitelijk misbruik.[1] Tegelijk kan men ook per ongeluk in bezit komen van kinderporno, zoals door ongevraagde post (*spam*), of doordat anderen gebruik maken van het nog al te vaak onvoldoende beveiligde draadloze netwerk van betrokkenen. De verbreding naar het internet leidt ook tot «zelfbeslachtoffering», doordat kinderen uit zichzelf of daartoe uitgedaagd, seksuele afbeeldingen van zichzelf verspreiden, zonder daarvan de risico's te onderkennen.[2]

Belang en benadering

Over de aanpak van kinderpornografie, en breder de inhoud en handhaving van de zedelijkheidswetgeving, is geregeld overleg met uw Kamer. In het laatst gehouden Algemeen Overleg[3] is vastgesteld dat zowel de kamer als de regering een krachtige aanpak voorstaan. Niet alleen in Nederland, ook in andere landen is er een brede consensus dat kinderpornografie en seksueel kindermisbruik een harde aanpak verdienen. Die aanpak zal, gegeven de veranderde kenmerken en daarmee vergrote diversiteit van het fenomeen, bestaan uit een meersporenbeleid.[4]

Preventie

Het kabinet heeft al verschillende initiatieven genomen ter voorlichting aan burgers en bedrijven over risico's (campagnes zoals *digibewust*). Er ligt immers een grote verantwoordelijkheid bij ouders om pornografie weg te houden van hun kinderen maar ook om te voorkómen dat «pedofiele roofdieren» ze lokken. Dat kan door het vermijden van bepaalde sites op internet of het installeren van filters op de eigen computerapparatuur. Dergelijke op ondersteuning van preventie gerichte overheidsinspanningen worden voortgezet en waar mogelijk geïntensiveerd, bijvoorbeeld door versterking van initiatieven in het onderwijsveld zoals het in 2007 uitbrengen van een stripboek over de gevaren voor kinderen op internet van (Suske en Wiske: *De Sinistere Site).* Daarnaast wordt de steun doorgezet aan niet-gouvernementele instellingen zoals het particuliere meldpunt kinderpornografie dat naast voorlichting een forum biedt aan burgers en bedrijven om melding te doen van kinderpornografie, naast de bestaande kanalen van politie hiervoor.
Op *chatsites* is het steeds meer gebruikelijk dat men werkt volgens protocollen die onder andere voorzien in het begeleiden («modereren») van gespreksgroepen. Dit heeft echter slechts een beperkt effect: een substantieel deel van het chatverkeer op internet vindt plaats in zogenoemde *instant messaging-systemen* die naar hun aard niet aan moderatie onderhevig zijn. Hiervan kan dus niet teveel aan bescherming worden verwacht. Een steeds weer terugkomende vraag bij dit onderwerp is in hoeverre de overheid een rol dient te vervullen in deze omgevingen. Vooralsnog is de keuze om hier geen preventieve aanwezigheid te verzorgen, maar te vertrouwen op het gezonde verstand en initiatief van de direct betrokkenen (w.o. ouders).

De aanpak van websites met kinderpornografische afbeeldingen

De politie komt websites met kinderpornografisch materiaal op het spoor door de meldingen via de daarvoor ingestelde meldpunten (het particuliere meldpunt kinderporno op internet en het meldpunt cybercrime van de Nederlandse politie), of via meldingen van politiediensten uit andere landen, of door zelf hier te surveilleren.
Zelfregulering en publiek-private samenwerking zijn, als pro-actieve benadering, ook voor de bestrijding van kinderpornografie van belang. Providers zijn in Nederland al langer actief in het weren van kinderpornografie. Maar het meeste kinderpornografisch materiaal komt van elders, van

[1] Carr, op. cit. p. 21.
[2] Zie bijv. Jaarverslag 2005 van de Stichting Meldpunt ter Bestrijding van Kinderporno op internet. Amsterdam, april 2006.
[3] Tweede Kamer, vergaderjaar 2007–2008, 31 200 VI, nrs. 9, 85 en 101.
[4] Zie Stol op. cit., Carr, op. cit. en Albert Benschop. Regulatie van CyberPorno – Morele en technologische filters, sociale controle en strafrechtelijke vervolging. (www2.fmg.uva.nl/websoc/regulatieporno.html).

buiten de EU, vaak uit landen waar de desbetreffende afbeeldingen of niet (of anders) strafbaar zijn of waar men weinig prioriteit geeft aan de bestrijding ervan. In de steeds weer opkomende discussies over de mogelijkheden om vanuit Nederland te zorgen voor verwijdering en of ontoegankelijk maken van websites met kinderpornografisch materiaal voor gebruikers van het internet, zijn een aantal zaken te onderscheiden.
Degene die kinderpornografische afbeeldingen op internet wil verspreiden gebruikt gewoonlijk één van de volgende drie manieren. Via het netwerk van een (Nederlandse) Internet Service Provider (ISP) wordt door een abonnee een website ingericht. Ook kan via zogenaamde hostingbedrijven in Nederland of elders op de wereld serverruimte worden gehuurd waarop men zelf vervaardigde, te onderhouden en te beheren websites kan plaatsen.
Daarnaast is het mogelijk om rechtstreeks via het internet bestanden met derden uit te wisselen.
Verspreiding vanuit Nederland via een Nederlandse ISP of hostingprovider is aan te pakken, enerzijds via strafrechtelijke weg en anderzijds via de private weg door de website fysiek uit de lucht halen. De Nederlandse ISP's en hostingbedrijven werken over het algemeen goed samen met de politie en verwijderen een website met kinderpornografisch materiaal als de politie de providers van de aanwezigheid van een dergelijke site in hun netwerk op de hoogte stelt. In een groot aantal landen op de wereld gebeurt dit op vergelijkbare wijze. Informatie over buitenlandse websites met kinderpornografisch materiaal die vanuit Nederland zijn vastgesteld, wordt door het Korps Landelijke Politie Diensten (KLPD) aan die landen gemeld.

In de praktijk blijkt dat aanbieders van kinderpornografie voortdurend inspelen op de door de overheden getroffen maatregelen. Het (veelvuldig) wisselen van hostingproviders wereldwijd door de professionele aanbieders van dergelijke kinderpornografie, bemoeilijkt het actueel houden van zogenaamde zwarte lijsten die in een aantal landen waaronder Nederland worden gebruikt. Dit kan verklaren waarom bij Nederlandse hostingbedrijven buitenlandse sites met kinderpornografie terug te vinden zijn.
Het verwijderen van kinderpornografie op websites die komen vanuit landen waar geen actie ondernomen wordt tegen dit soort misdrijven is niet vanuit Nederland mogelijk. In andere landen is daarvoor beleid ontwikkeld om te komen tot blokkering van deze sites via de lokale providers. waardoor bepaalde kinderpornografische internetadressen niet meer benaderbaar zijn voor hun klanten (dit is een zogenaamde omleiding naar een *STOP-pagina*). In Nederland is daar in 2007 mee gestart op initiatief van het KLPD. Enkele providers doen dit al met succes, op basis van een afgesloten convenant met het KLPD, die een lijst met te blokkeren sites aanlevert. In het Algemeen Overleg met uw Kamer over de zedelijkheidswetgeving en de aanpak van kinderpornografie op internet[1] is de stand van zaken als het gaat om het blokkeren van kinderpornografiesites, uitvoerig aan de orde geweest. Toen gaf ik aan dat ik tot het einde van 2007 zou afwachten of het KLPD en de nog niet meewerkende providers hier samen een oplossing zouden kunnen vinden. Eind december 2007 was onvoldoende voortgang hierin geboekt. Vanuit mijn departement is de afgelopen periode nader overleg gevoerd zowel met het KLPD als met een aantal providers. Dit positief verlopen overleg heeft ervoor gezorgd dat de partijen inmiddels tot elkaar zijn gekomen en op korte termijn zullen er meer providers zijn die op basis van de lijst met te blokkeren sites van het KLPD overgaan tot blokkeren.
Overigens zal in het tweede kwartaal van dit jaar het rapport van het WODC-onderzoek over de effectiviteit van filteren worden afgerond, waarover ik uw Kamer nader zal informeren.

[1] Tweede Kamer, vergaderjaar 2007–2008, 31 200 VI, nrs. 9, 85 en 101.

Strafrecht

De afgelopen jaren is de zedelijkheidswetgeving aangepast en is in onderling overleg[1] vastgesteld dat die aanpassing effectief is gebleken. Wezenlijk voor de internationale samenwerking is dat ook in het buitenland de zedelijkheidswetgeving op peil is of wordt gebracht.[2] Recent is de internationale harmonisering weer een stap verder gekomen door de ondertekening in Lanzarote van het nieuwe verdrag van de Raad van Europa tegen seksuele exploitatie en seksueel misbruik van kinderen. Zoals al is aangekondigd is de daarvoor nodige aanpassing van de Nederlandse wetgeving in voorbereiding – dit zal medio 2008 leiden tot indiening. Daarmee zal het hiervoor genoemde *hawking/grooming* strafbaar worden, alsook het onder omstandigheden zich toegang verschaffen tot kinderpornografisch materiaal (zonder dit op de eigen computer te downloaden) strafbaar zijn. Ter bestrijding van kinderpornografie is in de afgelopen jaren een actief beleid van opsporing en vervolging ontwikkeld, getuige ook de in 2007 herziene beleidsregels van het Openbaar Ministerie (Stcrt. 2007, 79 en 162). Dat dit effect heeft, blijkt uit de toenemende gevallen van ontmanteling van kinderpornografische (ICT-)netwerken, waarbij vele landen eendrachtig samenwerkten. Mede hierdoor wijken kinderpornografen steeds vaker uit naar versleutelingstechnieken, en meer en meer vindt uitwisseling plaats tussen pedofielen via aparte, besloten elektronische netwerken (*peer-to-peer networking*).[3] Dit is gunstig vanuit het oogpunt van vermindering van algemene blootstelling aan kinderpornografisch materiaal, doch het impliceert wel dat sneller ook bijzondere opsporingsmethoden nodig kunnen zijn om een effectieve aanpak mogelijk te maken.

Voortgang

Het beleid zoals dat met de Tweede Kamer is besproken, waarbi diverse ideeën zijn geopperd en met moties ondersteund, zal het kabinet met verve uitvoeren. Toegezegd is op concrete punten resultaten te bereiken, over de voortgang hiervan zal ik binnenkort een afzonderlijke brief naar de Kamer sturen. De bestrijding van kinderpornografie zal onderdeel zijn van de bovengenoemde proeftuinen vanuit het programma bestrijding cybercrime.

V.2 De aanpak van radicale uitingen en terroristische informatie

Gebruik van internet

In zijn rapport *Jihadisten en het internet* (december 2006)[4] bespreekt de Nationaal Coördinator Terrorismebestrijding (NCTb) de dreigingen die voortkomen uit het gebruik van internet door jihadistische terroristen en radicalen (jihadisten). In deze fenomeenstudie wordt onderscheid gemaakt tussen het gebruik van het internet als doelwit, als wapen en als middel. De kans dat de vitale (ICT-)infrastructuur als zodanig onderwerp is van aanslagen wordt niet waarschijnlijk geacht. Ook cyberaanvallen via het internet met een terroristisch oogmerk zijn niet waarschijnlijk. Het gebruik van het internet als doel en als wapen krijgt op deze plaats geen verdere behandeling- de bescherming van de vitale infrastructuur krijgt in het bijzonder uitwerking via het op 8 november 2007 opgerichte Nationaal Adviescentrum Vitale Infrastructuur (NAVI).

Hier gaat de aandacht in het bijzonder uit naar het door de NCTb als omvangrijk aangeduide gebruik van internet als middel voor de versterking van het terrorisme door propageren van de radicale boodschappen mede door het vormen van virtuele netwerken gericht op jongeren. Dat dient rekruterings- en trainingsdoeleinden. Hoezeer internet hierin een rol kan vervullen, kan worden geïllustreerd met het verspreiden van beelden

[1] Tweede Kamer, vergaderjaar 2007–2008, 31 200 VI, nrs. 9, 85 en 101.
[2] Zie het Kaderbesluit 2004/68/JBZ, ter bestrijding van seksuele uitbuiting van kinderen en kinderpornografie dd. 22 december 2003. En breder de artikelen 34 en 19 van de United Nations Convention of the Rights of the Child.
[3] Carr, op. cit. p. 25; Benschop, op. cit.; Van der Zee en Groeneveld, op. cit. p. 240. Er zijn schattingen, voor wat het waard is, dat tussen de 50 000 en 100 000 pedofielen betrokken zijn bij georganiseerde pornografiekringen in de hele wereld, waarvan een derde in de USA Wortley and Smallbone, op cit.
[4] Tweede Kamer, vergaderjaar 2006–2007, 29 754 nr. 95.

via internet door A-Zarqawi van beelden van een onthoofding van een Amerikaanse gijzelaar in 2004. Dit creëerde meer aandacht van vriend en vijand en ondermijnde de USA-plannen meer dan het opblazen van 100 mensen in Najaf – tegelijk maakt hij zich hiermee tot held tot alle jihadisten in de wereld.[1] Bij het gebruik van het internet als middel moet verder gedacht worden aan het plannen en voorbereiden van terroristische activiteiten, het gebruik ervan als een handelsplaats voor wapens, explosieven of grondstoffen of voor het maken van explosieven door het verspreiden van instructies of handleidingen. Ook kunnen plattegronden en of andere aanwijzingen uitgewisseld worden ter voorbereiding van terroristische aanslagen. Daarnaast is het internet bij uitstek het medium voor haatzaaiuitingen, opruiing, bedreigingen en radicaliserende boodschappen. Een dergelijk gebruik is, hoezeer dit heden ten dage ook in het oog springt, helaas niet voorbehouden aan de politieke islam. Ook andere radicale groepen kunnen immers van de moderne communicatiemiddelen gebruik maken, of het nu gaat om nazistische groepen, antigloblisten of dierenrechtactivisten. Het is dus een breder perspectief waarbinnen het voornemen bestaat, zoals geuit in het coalitieakkoord, om *radicaliserende boodschappen en voorlichting over de middelen van terreur te bestrijden.* Dit voornemen is leidend in de aanpak van terroristische informatie op of via het Internet, naast de hieronder geschetste internationale belangen.

Internationale context

De aanpak met betrekking tot het tegengaan van radicale uitingen en voorlichtingsmateriaal loopt in lijn met het internationaal voorgestane beleid. Het *Europees Verdrag ter voorkoming van terrorisme*[2] verplicht tot strafbaarstelling van oproepen tot terrorisme, terroristische training en rekrutering, als ook het verspreiden van handleidingen voor het maken van explosieven. De Europese Commissie heeft een voorstel gedaan tot uitbreiding van het *Kaderbesluit terrorisme* van 13 juni 2002 met de strafbaarstelling van het publiekelijk uitlokken tot het plegen van een terroristisch misdrijf, het werven voor terrorisme en het trainen voor terrorisme, ook als deze gedragingen via het internet worden gepleegd. Voorts heeft de Europese Commissie in zijn mededeling voor een Europese aanpak van cybercrime (22 mei 2007) het internetgebruik voor terroristische doeleinden als één der aandachtsgebieden benoemd met nadruk op samenwerking tussen de publieke en private sector bij het blokkeren van boodschappen. Daarnaast wordt geïnvesteerd in het EU-project «Check the Web»; een samenwerkingsverband waarin lidstaten informatie uitwisselen van internet analyses die verkregen zijn op basis van monitoring via het informatieportal ondergebracht bij Europol. Tot slot zij gewezen op de «Counter Terrorism Implementation Task Force» dat in het kader van de uitvoering van de VN Strategie ter bestrijding van terrorisme is opgericht en zich onder andere richt op de uitvoering van maatregelen op het terrein van internetgebruik door terroristen[3]. Internationale samenwerking en een gemeenschappelijke internationale aanpak van terroristische informatie op het internet wordt zeer essentieel gevonden. De Nederlandse maatregelen en acties die hierna aan de orde komen zijn enerzijds een invulling van de passage uit het coalitieakkoord en anderzijds een uitwerking van internationale wet- en regelgeving en beleid, waarin Nederland veelal een voortrekkersrol vervuld.

Reikwijdte van het tegenhouden van radicaliserende boodschappen en voorlichtingsmateriaal

De Nederlandse focus ligt enerzijds op het signaleren en anderzijds op het tegengaan van verspreiding van boodschappen en informatie door internetpartijen. Evident is dat hierbij uitgegaan moet worden van het grondwettelijke recht op vrijheid van meningsuiting: artikel 7 van de Grondwet

[1] Paul Eedle. Al/Qaeda's Super Weapon: The Internet. Paper presented at the Conference 'Al/Qaeda 2.0: Transnational Terrorism After 9–11 (Washington 1–2 December 2004).
[2] Trb. 2006, 34.
[3] Project met een looptijd van 1 jaar (2008) dat gefinancierd wordt door de NCTb en het Ministerie van Buitenlandse Zaken.

zegt dat burgers vrij zijn in het uiten van hun gedachten en dat zij zonder beperking kennis kunnen nemen van gedachten en gevoelens van anderen. De overheid dient zicht te onthouden van censuur en mag andere organen of bedrijven ook niet verplichten tot censuur. Alleen als sprake is van een strafbare uiting mag de overheid ingrijpen. Verdragsrechtelijk is de vrijheid van meningsuiting neergelegd in artikel 10 EVRM. Er bestaat op basis van deze bepaling pas een noodzaak tot inperking van die vrijheid van meningsuiting als er een *pressing social need* is, waarvan de noodzaak overtuigend moet worden vastgesteld. Daarnaast gelden de beginselen van proportionaliteit en subsidiariteit.

De meeste uitingen vallen daarmee onder de vrijheid van meningsuiting, tenzij er sprake is van evidente schending van de rechtsnorm (zoals overtreding art. 137d Sr). De Hoge Raad accepteert bijvoorbeeld dat de strafbaarheid bij discriminatoire uitlatingen vervalt, als deze hebben plaatsgevonden in een context die bijdraagt aan het maatschappelijk debat of die anderszins van een zekere functionaliteit getuigt. Indien echter een uitlating in nodeloze agressieve of grievende bewoordingen is vervat of de toonzetting ervan de grenzen van aanvaardbare polemiek overschrijdt, kan wel sprake zijn van strafbaarheid en kan er strafrechtelijk tegen worden opgetreden. Deze randvoorwaarden maken dat politie en justitie tot op heden terughoudend zijn in de opsporing en vervolging van dit soort zaken, nog versterkt doordat niet altijd makkelijk valt te achterhalen wie wat waar heeft gezegd en welke jurisdictie geldt. Het aangekondigde actievere strafrechtelijke anti-discriminatiebeleid[1] zal de jurisprudentie moeten opleveren die als richtsnoer geldt voor de toekomst.

Artikel 7 van het Verdrag van de Raad van Europa ter voorkoming van terrorisme bepaalt dat partijen maatregelen nemen die nodig zijn om *training voor terrorisme* als strafbaar feit aan te merken in haar nationale regelgeving. Hieronder wordt verstaan *«het geven van instructie voor het vervaardigen of gebruiken van explosieven, vuurwapens of andere wapens of schadelijke of gevaarlijke stoffen, of voor andere specifieke methodieken of technieken, met als doel het plegen van of bijdragen aan het plegen van een terroristisch misdrijf, in de wetenschap dat beoogd wordt de verstrekte vaardigheden daarvoor in te zetten»*. Nederland heeft dit Verdrag ondertekend en werkt aan ratificatie. De wetgeving ter implementatie van het Verdrag is in maart 2008 bij de Tweede Kamer ingediend[2] en het wetsvoorstel ter goedkeuring van het Verdrag in april 2008.[3] De voorgestelde regeling leidt tot strafbaarstelling van het opzettelijk en wederrechtelijk verspreiden van voorlichtingsmateriaal tot het (vergemakkelijken van het) plegen of voorbereiden van een terroristisch misdrijf.

In lijn met dit Verdrag van de Raad van Europa heeft de Europese Unie een voorstel gedaan voor een kaderbesluit tot wijziging van het kaderbesluit 220/475/JBZ inzake bestrijding van terrorisme. De aanpassing ziet – mede in het licht van het toegenomen en veranderde gebruik van internet door terroristen – onder andere op de strafbaarstelling van het trainen voor het plegen van een terroristisch misdrijf.

Monitoring en surveillance

Monitoring en surveillance[4] zijn vanaf 2006 projectmatig opgepakt door de NCTb en het KLPD, in nauwe afstemming met de AIVD en de MIVD, passend bij ieders eigen verantwoordelijkheid en taakstelling.
De NCTb heeft radicaal-islamitische uitingen en gedragingen op een aantal Nederlandstalige en buitenlandse sites gevolgd, en kennis en inzicht ontwikkeld met betrekking tot de mogelijkheden van het doen van onderzoek op het internet, technische zoekprogramma's alsmede met betrekking tot een doelmatige en veilige opslag van gegevens. Daarmee is

[1] De strafrechtelijke aanpak van discriminatie moet worden verbreed, volgens de Minister van Justitie zijn reactie op het WODC-onderzoek «Strafbare discriminatie». Tweede Kamer, vergaderjaar 2007–2008, 31 200 VI, nr. 97. Eerder al benoemde het College van procureurs-generaal het tegengaan van discriminatie al tot prioriteit (in het meerjarenplan Perspectief op 2010).
[3] Tweede Kamer vergaderjaar 2008–2009, 31 422, nr. 2.
[4] Zie noot 1, pagina 10 voor het onderscheid tussen surveillance en monitoring.

een basis gelegd voor het oog houden op de mate waarin radicale en terroristische boodschappen op internet verspreid worden. Dit monitoren is van belang gebleken voor het opstellen van rapportages over actuele ontwikkelingen, lange termijn fenomeenstudies en verdiepende analyses. Het monitoren van het internet is inmiddels structureel ingebed in de NCTb-organisatie, waarbij op reguliere basis afstemming plaatsvindt met de betrokken partijen KLPD, AIVD en MIVD.

Het KLPD surveilleert op het internet teneinde meer zicht te krijgen op radicale uitingen en terrorismegerelateerde activiteiten op het internet. Er zijn in dat kader sites geselecteerd die structureel en systematisch worden gevolgd, met een radicaal-islamitische, rechts-extremistische en links-activistische signatuur. In een aantal gevallen is er strafbare informatie aangetroffen waarnaar een strafrechtelijk onderzoek wordt verricht. Er zijn gedurende het project tevens strafbare feiten ontdekt die buiten de scope van het project vallen.[1] Deze «bijvangst» is doorgezet naar de betrokken regiokorpsen. Tevens zijn regiokorpsen ingeseind over mogelijke dreigingen (naar aanleiding van demonstraties) en is er ervaring opgedaan met het veilig en (on)opvallend zoeken en volgen op het internet. In het voorjaar van 2008 zullen de resultaten van het surveillanceproject aan mij voorgelegd worden. Zoals eerder genoemd maakt surveillance onderdeel uit van het Versterkingsprogramma bestrijding cybercrime.

Meldpunt Cybercrime

Sinds 2006 is het Meldpunt Cybercrime (MCC) actief. Doel van het MCC is te komen tot een centrale online voorziening waar burgers en bedrijven alle mogelijke vormen van cybercrime kunnen melden, ter vergroting van zicht op aard en omvang van in Nederland voorkomende vormen van cybercrime en het bevorderen van maatregelen ter bestrijding van de verschillende cybercrimevormen. Vooralsnog kan er melding gedaan worden van kinderpornografie en terrorisme.[2] In hoeverre een uiting of informatie op het internet terrorisme, haatzaaien of radicalisering betreft, blijkt voor de burger zeer lastig in te schatten. De komende periode zal het MCC activiteiten initiëren met als doel meer informatie te verstrekken over deze criminaliteitsvorm en uitingen hiervan op het internet. De verwachting is dat het aantal meldingen dienaangaande zal toenemen.
Er vindt onder andere samenwerking plaats tussen het MCC en het surveillanceteam van het KLPD, opdat waar nodig informatie wordt uitgewisseld en de nodige opvolging plaatsvindt. In het voorjaar wordt de werking van het MCC geëvalueerd. Gestreefd wordt naar doorontwikkeling van het MCC en een grotere bekendheid van het meldpunt door bijvoorbeeld uitbreiding van te melden vormen van cybercrime.

Notice-and-Take-Down, filteren en blokkeren

In hoofdstuk IV is al uitgebreid aandacht besteed aan de noodzaak te komen tot een NTD-systematiek op basis van zelfregulering, naast een adequate bevelsstructuur op grond van artikel 54a Sr.
Ook is al gewezen op de mogelijkheid tot het filteren en blokkeren van informatie afkomstig uit het buitenland door Nederlandse ISP's. De ontwikkelingen met betrekking tot filteren en blokkeren worden nauwlettend gevolgd. Daarbij is het volgende van belang: in tegenstelling tot kinderpornografische afbeeldingen, is bij terrorisme-gerelateerde informatie niet altijd klip en klaar dat het om *strafbare* of onrechtmatige informatie gaat. De bereidheid van internetpartijen om informatie ontoegankelijk te maken geldt alleen ten aanzien van strafbare of onmiskenbaar onrechtmatige informatie. In de beoordeling of bepaalde radicaliserende uitingen strafbaar zijn of niet, geldt de huidige jurisprudentie als referentiekader. Zoals eerder vermeld, is deze vrij beperkt en contextueel van

[1] Zoals het aanbod van vuurwapens en explosieven, mishandeling en bedreigingen.
[2] van april 2007 tot en met februari 2008 zijn er in totaal 1145 meldingen binnengekomen bij het Meldpunt Cybercrime, waarvan 762 meldingen kinderpornografie betroffen, 120 terrorisme en 263 overig. Over de opvolging van de meldingen kunnen nog geen concrete resultaten worden afgegeven door het Meldpunt Cybercrime.

karakter. Dit heeft effect op de kans van slagen van het ontoegankelijk maken van terroristische uitingen. De vrijheid van meningsuiting zal onder deze omstandigheden prevaleren boven het tegengaan van «radicaliserende (niet strafbare) boodschappen».
Verder zij nog gewezen op het belang van opsporings- of inlichtingen- en veiligheidsdiensten tot het *online* houden van bepaalde terrorisme-gerelateerde informatie ten behoeve van het opsporingsonderzoek of inlichtingenwerk. Dit vergt waar mogelijk steeds afstemming tussen betrokken diensten en partijen.

V.3 Illegaal gokken

Het verschijnsel

Internetgokken is een sterk groeiende bedrijfstak waarin miljarden omgaan, via duizenden sites, met miljoenen deelnemers. In sommige landen en staten is internetgokken toegestaan, in andere is dit verboden. Veel sites zijn gevestigd in landen die daar economisch voordeel in zien zoals Antigua en Costa Rica. Kortweg stelt men dat *«miljoenen .. gokken iedere dag online zonder de bescherming van betrouwbare regulerende structuren die op leeftijd en identiteit controleren, die zorgen voor integer en eerlijk spel*».[1]
De zorgen over het illegaal gokken op internet komen ten eerste voort uit de drempelverlaging die daarmee annex is: het casino staat in de huis- of slaapkamer. Daarmee is het gokken direct en dagelijks toegankelijk voor iedereen, dus ook voor jongeren. Voorts blijft probleemgokken achter de computer buiten beeld tot het te laat is. Ten tweede vormt de context van het internetgokken een prachtige gelegenheid voor bedrijven om de klant te bedriegen. Zo kunnen zij immers bepalen welke kaarten er met pokeren worden uitgedeeld, waarmee ze in beginsel in staat zijn hun eigen winstkansen te regelen en beïnvloeden. Tenslotte zou, overigens net als nu al het geval is in het gokwezen, het internetgokken kunnen helpen bij het witwassen van illegaal verkregen geld en daarmee de doelen van criminele of zelfs terroristische organisaties kunnen dienen.

Regulering

Het via Internet gelegenheid geven tot deelname aan kansspelen is op dit moment onvoorwaardelijk verboden in Nederland: de Wet op de kansspelen voorziet niet in de mogelijkheid vergunningen daarvoor te verlenen. Uit regelmatig gehouden onderzoeken blijkt echter dat Nederlandse consumenten in toenemende mate ingaan op – dikwijls niet (in Nederland) gereguleerd – kansspelaanbod via Internet. Deze ontwikkeling heeft geleid tot een reactie van de Overheid, waarbij enerzijds een legaal kansspelaanbod via Internet zou worden geïntroduceerd en anderzijds de aanpak van illegale kansspelen via Internet wordt geïntensiveerd. Omdat nog niet kon worden overzien welke gevolgen dergelijk kansspelaanbod heeft op de kansspelverslaving en of de consument voldoende wordt beschermd, werd voorlopig gekozen voor een proef voor beperkte duur (maximaal drie jaar), met één aanbieder (Holland Casino). Aan dit experiment zouden strenge voorwaarden zijn verbonden opdat de potentiële risico's zoveel mogelijk beheerst kunnen worden. Na evaluatie van de proef zou worden besloten of en in welke omvang structureel aanbod van kansspelaanbod via Internet wordt toegestaan. De proef vereiste een (partiële) wijziging van de Wet op de kansspelen. Door de regering is hiervoor een wetsvoorstel ingediend. Dit wetsvoorstel is echter op 2 april 2008 door de Eerste Kamer verworpen. De consequenties hiervan voor het in gang gezette beleid worden nader onderzocht.

[1] Zie bijv. David O. Stewart Ropes and L.L.P. An Analyses of Internet. Gambling and its Policy Implications. American Gaming Association, 2006 (citaat vertaald).

Rechtshandhaving

Op basis van het beleidsplan «Aanpak bestrijding van kansspelen via Internet», dat op 16 september 2005 aan de Kamer is aangeboden (TK 24 557, nr. 59), is de afgelopen jaren een begin gemaakt met de aanpak van illegale Internetkansspelen. De aanpak behelst ten eerste het ontwikkelen van instrumenten en hulpmiddelen om illegaal aanbod en bemiddeling op te sporen en te komen tot vervolging, ten tweede het ontmoedigen van aanbod van, bevorderen van en deelname aan illegale kansspelen via internet door het voeren van een actief voorlichtingsbeleid, ten derde et aanpakken van illegale aanbieders en tussenpersonen op basis van bestuursrecht, fiscaal recht, civiel recht en strafrecht.
Het Ministerie van Justitie heeft de afgelopen jaren een groot aantal in Nederland gevestigde aanbieders van illegale kansspelen en tussenpersonen gewaarschuwd dat zij in strijd met de Wet op de kansspelen handelen. Ongeveer 60 procent van de aangeschreven bedrijven heeft daaraan gevolg gegeven en heeft hun sites onbereikbaar gemaakt of aangepast. Het overige deel van de aanbieders heeft het illegale aanbod echter voortgezet, al dan niet vanuit het buitenland (of door inschakeling van buitenlandse tussenpersonen).
Ook in het buitenland gevestigde aanbieders en tussenpersonen dienen zich aan de in Nederland geldende wet te houden. De opsporing en vervolging van aanbieders van kansspelen via internet en hun tussenpersonen die in het buitenland gevestigd zijn, is overigens wel een knelpunt. Dergelijke organisaties, of hun servers, zijn veelal gevestigd in landen waar het organiseren van kansspelen niet strafbaar is gesteld of waar nauwelijks sprake is van regulering of toezicht op kansspelen.

Het financiële aangrijpingspunt in de handhaving

Aangezien een deel van de in Nederland gevestigde aanbieders en tussenpersonen, ondanks waarschuwingen vanuit het ministerie, het illegale aanbod continueert en omdat de aanpak van in het buitenland gevestigde aanbieders en tussenpersonen een knelpunt vormt, richt de aanpak ter bestrijding van illegale kansspelen via internet zich nu mede op financiële tussenpersonen, banken en creditcardmaatschappijen.
Het Ministerie van Justitie is al geruime tijd in overleg met de Nederlandse Vereniging van Banken (NVB) om afspraken te maken over de wijze waarop, de omstandigheden waaronder en de juridische waarborgen waarbinnen financiële instellingen contracten met binnen- en buitenlandse organisaties die kansspelen via internet aanbieden kunnen weigeren of verbreken. Het Ministerie van Justitie zal de NVB voorzien van een «zwarte lijst» met organisaties die zonder vergunning gelegenheid geven tot deelname aan kansspelen via internet en daarmee de Wet op de kansspelen overtreden. De zwarte lijst wordt samengesteld op basis van openbare (via het internet te verkrijgen) informatie.
De NVB zal de lijst ter beschikking stellen van de banken, zodat deze de desbetreffende rekeningen kunnen opzeggen of weigeren. Deze aanpak richt zich uitsluitend op de organisaties die gelegenheid tot deelname aan kansspelen via internet geven en niet op consumenten. Het verstrekken van een rekening aan een aanbieder van kansspelen via internet is op grond van de Wet op de kansspelen en de Wet op het financieel toezicht niet toegestaan. Banken mogen op basis van de integriteitbepalingen, het «ken uw klant» beleid (*Cliënt Due Diligence*) en jurisprudentie geen rekening verstrekken aan aanbieders van kansspelen via internet. Als een Nederlandse bank de dienstverlening aan een zakelijke rekeninghouder beëindigt, dan eindigt automatisch ook bijvoorbeeld een iDEAL contract, evenals eventuele incassocontracten, kredietfaciliteiten, en dergelijke.
Niet alleen financiële instellingen, maar ook providers zullen op hun verantwoordelijkheid worden aangesproken. De providers kunnen op

eigen initiatief of op verzoek van derden het illegale aanbod ontoegankelijk maken (verwijderen of blokkeren). Hierin spelen providers al een actieve rol: er zijn NTD-procedures waarbij klanten kunnen ageren tegen (vermeend) onrechtmatige uitingen. Ook politie en justitie kunnen de provider hierop wijzen. Een dergelijke signalering heeft vaak een positieve actie tot gevolg: providers spelen hiermee al een belangrijke rol op grond van een zelf gevoelde verantwoordelijkheid.

V.4 Auteursrecht

Nog veel verspreiding

De bescherming van intellectueel eigendom heeft met de komst van internet een extra dimensie gekregen. Vergeleken met de mogelijkheden van de banden en videorecorder in de jaren '60 en '70 is het tegenwoordig op ongekende wijze mogelijk om door het auteursrecht en de naburige rechten beschermde werken vrijelijk uit te wisselen. Intussen heeft zich een zekere sanering afgetekend, door de civielrechtelijke acties tegen sites die het mogelijk maakten onbelemmerd ook beschermde muziekbestanden aan te bieden (illegaal *uploaden*). Was er voorheen nauwelijks een legaal alternatief, sinds een aantal jaren zijn er al veel gebruikte sites opgericht die online verkoop van muziek, films, games en software tegen betaling verzorgen. Ook worden er steeds geavanceerdere technieken ingezet om auteursrechtelijke inbreuken te voorkomen (o.a. filtering, fingerprinting en drm-technieken). Dit alles laat onverlet, dat nog veelvuldig sprake is van illegale verspreiding op internet van bestanden die vallen onder een intellectueel eigendomsrecht.

Uitgangspunten rechtshandhaving

In overeenstemming met de eerder in deze brief en in de beleidsbrief over het auteursrecht van 20 december 2007[1] gevolgde benadering, en in overeenstemming met het eerder al gecodificeerde beleid op dit punt[2] wordt uitgegaan van het primaat van de civielrechtelijke handhaving door de rechthebbende zelf bij de bestrijding van inbreuken op intellectuele eigendomsrechten. Daartoe biedt de privaatrechtelijke wetgeving op het gebied van de intellectuele eigendom voldoende maatregelen en procedures zoals het uit de handel halen en vernietiging van de illegale producten, het vorderen van schadevergoeding en winstafdracht en het opleggen van dwangsommen ter voorkoming van toekomstige overtredingen. Ook kan een auteursrechthebbende ten behoeve van het achterhalen van de daadwerkelijke inbreukmaker vorderen dat een tussenpersoon, zoals een internet service provider, de naam adres woonplaatsgegevens (naw) van de inbreukmakende afnemers van diens diensten (bijv. de websitehouder) verstrekt. Op basis van recente jurisprudentie van het Hof van Justitie[3] dient daarbij een evenwichtige en zorgvuldige belangenafweging plaats te vinden tussen privacybescherming en de handhaving van intellectuele-eigendomsrechten, in het licht van de concrete omstandigheden van het geval. Richtinggevend voor de Nederlandse situatie is daarbij het arrest Lycos/Pessers van de Hoge Raad van 25 november 2005[4] Op grond hiervan is een serviceprovider tot verstrekking van naw-gegevens gehouden als sprake is van (mogelijke) onrechtmatigheid, schade, er geen minder ingrijpende manier openstaat en het belang van de rechthebbende zwaarder weegt dan het privacybelang van de abonnee.[5] Om deze civielrechtelijke aanpak effectiever te maken, hebben rechthebbenden zich veelal georganiseerd in privaatrechtelijke organisaties die hun belangen vertegenwoordigen. Deze organisaties verzorgen het contact met de opsporingsinstanties die de strafrechtelijke handhaving voor hun rekening nemen.

[1] Tweede Kamer, vergaderjaar 2007–08, 29 838, nr. 6.
[2] College van procureurs-generaal: Aanwijzing intellectuele eigendomsfraude en de Richtlijn voor strafvordering intellectuele eigendomsfraude (Stcrt 2006, 6; datum inwerkingtreding 01–02–2006).
[3] 29 januari 2008, C-275/06 Promusicae/ Telefónica de Espaáa SAU.
[4] Hoge Raad, RvdW 2005, 133.
[5] Zie hierover uitgebreider mijn brief van 20 maart 2008, Kamerstukken II 2007/08, 29 838, nr. 7.

De strafrechtelijke handhaving komt bij dit onderwerp in beeld indien het algemeen belang dit vordert. Het strafrecht zal in stelling worden gebracht bij zodanig grootschalige piraterij, die de markt ernstig verstoort, dat deze doormiddel van privaat optreden niet voldoende kan worden bestreden, of bij betrokkenheid van georganiseerde criminaliteit. Bij dit laatste gaat het erom dat de inbreuk op het intellectuele eigendomsrecht zodanig is georganiseerd, of zozeer stelselmatig wordt gepleegd, dat het strafrecht als enige zinvol denkbaar correctiemiddel overblijft.
Zoals al is aangegeven in de al eerder vermelde beleidsbrief van 20 december 2007 zal de strafrechtelijke handhaving van het auteursrecht zich concentreren op bestrijding aan de bron van het illegale aanbod op internet, namelijk op degene die grootschalig illegaal «uploadt» en daarmee films, games en muziek in strijd met het auteursrecht via internet aanbiedt. Daarmee zal het illegaal aanbod worden beperkt en het legaal aanbod meer kansen krijgen.

De handhaving van het auteursrecht kan mee profiteren van diverse in deze brief aangekondigde maatregelen en onderzoeken, zoals de analyse ten behoeve van de actualisering van het juridisch instrumentarium, de organisatorische voorzieningen zodat politie en justitie op adequate wijze op aangiften van cybercrime reageren en het onderzoek naar publiek-private samenwerking in het kader van een NTD-procedure. Om de zich voordoende mogelijkheden te benutten zal overleg worden bevorderd tussen de belangrijkste betrokken partijen zoals vertegenwoordigers van de film- en muziek industrie en het Openbaar Ministerie, de politie en de FIOD/ECD.
Zoals toegezegd in de brief aan de TK over het auteursrecht[1], worden in opdracht van het kabinet momenteel de economische en culturele effecten onderzocht van digitale verspreiding van auteursrechterlijk beschermd materiaal. Dit onderzoek zal naar verwachting in het najaar van 2008 gereed zijn.

V.5 Enige andere onderwerpen

In de voorafgaande paragrafen van dit hoofdstuk zijn een aantal belangrijke aan cybercrime gerelateerde criminaliteitvormen aan de orde gekomen. Hieronder worden enige andere kort besproken.

Prostitutie

Ook bij dit onderwerp komt internet aan de orde. In het najaar van 2008 kunt u, in het kader van de regulering van prostitutie, de indiening van een concept kaderwet verwachten. Daarin zal ook het aanbod van prostitutie via internet aan de orde komen. Momenteel wordt er nog gestudeerd op de mogelijkheid om dat te verbreden tot seksuele dienstverlening in het algemeen, waar het internet ook een belangrijke rol speelt.

Drugs

In het debat met uw kamer over het «Drugsbeleid in internationaal perspectief» op 6 maart 2008 heb ik u toegezegd de handhaving van het afficheringsverbod te zullen betrekken bij de aanpak van internetcriminaliteit. In het lopende WODC onderzoek naar handhaving en naleving van de coffeeshopcriteria zal mede gekeken worden naar dit onderwerp. Naar aanleiding van de uitkomsten daarvan zal in de drugnota die naar verwachting in april 2009 zal verschijnen zonodig een aanscherping plaatsvinden.

[1] Tweede Kamer, vergaderjaar 2007–2008, 31 200 VI, nr. 98, p. 14.

VI ONDERZOEK EN MONITORING

Zowel internationaal als nationaal is informatie over de aard, de omvang en de ontwikkeling van cybercrime en cybercriminelen alleen beperkt en fragmentarisch aanwezig. Gegeven de grote diversiteit van de criminaliteitvormen en typen van plegers, moet men niet te snel denken dat een omvattend beeld kan komen van een groot wetenschappelijk onderzoek. Wel lijkt het zinvol op hoofdlijnen te weten waar zich de dreigingen voordoen en welke vorm ze aannemen. Hiertoe worden enkele instrumenten ingezet. In 2008 komt er een zgn. nulmeting om een beeld te verkrijgen van de mate waarin in Nederland burgers en bedrijven te maken hebben met vormen van cybercrime. Deze zal een betrekkelijk uitvoerig inventariserend karakter dragen, waarbij ter wille van de vergelijkbaarheid aansluiting wordt gezocht met wat hieromtrent in andere landen al is gedaan (UK, USA, Australië). Op grond van die nulmeting zal een beperktere vraagstelling worden opgenomen in de bestaande instrumenten van de veiligheidsmonitoren (onder burgers respectievelijk bedrijven).
In aanvulling hierop zal op specifieke, kennelijk kwetsbare, deelterreinen nader onderzoek komen naar de kenmerken die kleven aan de desbetreffende criminaliteit, aan de omstandigheden waaronder men deze pleegt en aan de daarvoor verantwoordelijke daders. Bij de hierbij te vormen onderzoeksagenda zal getracht worden deze internationaal te verankeren, opdat kennis en ervaring gedeeld kunnen worden bij dit bij uitstek grenzeloos onderwerp.

VII SLOT

De ICT verandert patronen van de wijze waarop mensen met elkaar omgaan, al dan niet zakelijk. Hoe de samenleving daarvan profiteert, en hoe deze omgaat met de daaraan verbonden schaduwkanten, is een proces van evolutie. Bestaande concepten vragen om verbreding, verandering of vervanging om aan waargenomen ontwikkelingen tegemoet te komen respectievelijk het hoofd te bieden.
De benadering van de rechtshandhaving bij cybercrime zoals die in deze brief aan de orde is gekomen, is er in het bijzonder op gericht wezenlijke, diepliggende waarden te beschermen. Lang niet alles kan met overheidsregulering tegemoet worden getreden, burgers en ondernemingen kunnen zelf veel doen om hun veiligheid te waarborgen, wetgeving krijgt aanpassing waar dat nodig blijkt, in het strafrecht ligt de focus bij de bescherming van de vitale infrastructuur van de samenleving en van situaties waarin de essentiële belangen van burgers en bedrijven in de knel komen.
In een evolutionair proces zal bij voortduring de vraag aan de orde zijn of er genoeg verricht wordt. Omdat de ontwikkelingen maar beperkt te voorzien zijn, kan die vraag voor de toekomst niet op voorhand al een antwoord krijgen. Wel kan, zoals in deze brief is neergelegd, een kader worden geboden waarbinnen die vraag zinvol kan worden beantwoord. Hierin komt naar voren waar de (strafrechtelijke) overheid aan zet is en waar minder of niet. Uiteraard zal hierbij de vinger aan de pols moeten worden gehouden om vast te kunnen stellen óf er daadwerkelijk genoeg kan worden gedaan dan wel dat er een volgende stap moet komen in de regelgeving of het beleid.

De minister van Justitie,
E. M. H. Hirsch Ballin